UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SOFIA RECA and JAMES K. SUPPLES, Individually and on Behalf of All Others Similarly Situated,

Plaintiffs,

vs.

FLASHDOT LIMITED f/k/a PHOENIXFIN LIMITED, MEK GLOBAL LIMITED, PEKEN GLOBAL LIMITED, and PHOENIXFIN PRIVATE LIMITED (collectively d/b/a KUCOIN), CHUN (a/k/a "MICHAEL") GAN, KE (a/k/a "ERIC") TANG, and CHAINALYSIS, INC.,

Defendants.

Civil Action No. 1:24-cv-06316-GHW-SLC

CLASS ACTION

AMENDED COMPLAINT

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

Page

Page

Plaintiffs Sofia Reca ("Reca") and James K. Supples ("Supples," and with Reca, "Plaintiffs"), individually and on behalf of all others similarly situated, by and through their undersigned attorneys, bring this action against defendants Flashdot Limited f/k/a PhoenixFin Limited ("Flashdot"), Mek Global Limited ("Mek Global"), Peken Global Limited ("Peken Global"), and PhoenixFin Private Limited ("PhoenixFin"), together with Flashdot, Mek Global, and Peken Global, d/b/a KuCoin (collectively, "KuCoin"), Chun (a/k/a "Michael") Gan ("Gan"), Ke (a/k/a "Eric") Tang ("Tang," and with Gan and KuCoin, the "KuCoin Defendants"), and Chainalysis, Inc. ("Chainalysis") (collectively, "Defendants"). Plaintiffs allege the following based upon their own knowledge, or where there is no personal knowledge, upon the investigation of counsel and/or upon information and belief.

NATURE OF THE ACTION

1. Defendants Gan and Tang, through their ownership and association with defendants Flashdot, Mek Global, Peken Global, and PhoenixFin, formed and operate KuCoin, a major cryptocurrency exchange where customers deposit, trade, and withdraw hundreds of types of digital assets, including cryptocurrencies and tokens (collectively, "cryptocurrency" or "crypto"), such as Bitcoin ("BTC"), Ethereum ("ETH"), and others. Since its founding in September 2017 by defendants Gan and Tang, KuCoin has received and sent billions of dollars in crypto, with KuCoin receiving fees on every transaction. As of June 2024, KuCoin was the fifth-largest cryptocurrency exchange in the world. KuCoin's rapid growth was fueled, in large part, by KuCoin targeting the large and lucrative U.S. crypto market, and by ignoring and willfully violating numerous U.S. laws and regulations in place to protect consumers, investors, and American national security, which would have limited KuCoin's access to the U.S. market and slowed its growth.

2. Defendants, among other things, knowingly and admittedly failed to register as a money transmitting business ("MTB"), willfully violated the Bank Secrecy Act ("BSA") by failing

to implement and maintain an effective anti-money laundering ("AML") program, and disregarded crucial know-your-customer ("KYC") rules – all in a deliberate and calculated effort to profit from the U.S. market without implementing controls required by U.S. law.

3. Defendants' willful disregard of these important laws and regulations turned KuCoin into a magnet and hub for criminals, users from sanctioned jurisdictions, terrorists, and other bad actors, because KuCoin became a critical part of their effort to launder crypto that was stolen or obtained by other unlawful means. KuCoin became a preferred choice as the "get-away driver" for a large number of bad actors. By flouting KYC and AML laws, KuCoin was advertising to all criminals that it was a safe place for them to transfer cryptocurrency obtained through nefarious means without risk of being stopped or identified.

4. Under normal circumstances, a core attribute of cryptocurrency transactions is that there is a permanent record of those transactions on the public blockchain; and the chain-of-title of cryptocurrency is permanently and accurately traceable on that public blockchain, which acts as a "ledger." After a bad actor steals someone's crypto, the location of the stolen cryptocurrency is publicly available on the blockchain. As a result, there is a substantial risk the authorities would track the bad actor down by retracing his steps on the blockchain, and the bad actor would need to constantly look over his proverbial shoulder. Because Gan, Tang, and others at KuCoin put profits before the law, the KuCoin Defendants, through the operation of KuCoin, generated substantial amounts of proceeds by offering bad actors a way to launder stolen assets – thus removing the connection between the ledger and their digital assets so the digital assets would no longer be traceable. By sending stolen cryptocurrency to KuCoin, bad actors used the KuCoin centralized cryptocurrency exchange to render stolen crypto untraceable, so they could evade detection and

profit from their criminal activities. During the Class Period (defined below), KuCoin served as the vehicle for laundering billions of dollars of proceeds from criminal activities.

5. Had KuCoin complied with U.S. law, it could have assisted in the freezing, tracking and potential recovery of stolen assets. The KuCoin Defendants' refusal to implement important KYC and AML policies and procedures, however – in flagrant violation of U.S. laws and regulations – facilitated the laundering of stolen cryptocurrency and prevented the recovery of the stolen assets.

6. KuCoin acted as a depository for millions of dollars of cryptocurrency removed from the digital wallets, accounts, or protocols of individuals and entities targeted in, and located in, the United States as a result of hacks, malware, theft, or ransomware, including Plaintiffs and members of the Class (defined below). Defendants acted together in furtherance of a scheme to maximize revenues for KuCoin from all sources, including U.S.-based users, sanctioned users, criminals, crypto-thieves, and accounts and cryptocurrency wallets previously identified as being connected to illegal conduct. Defendants and co-conspirators operated the KuCoin Crypto-Wash Enterprise (defined below), which enabled bad actors to transfer assets generated through criminal activity that targeted victims located in the United States (including New York) to KuCoin, exchange those assets for different assets on KuCoin's exchange, and then transfer those newly "cleaned" assets out of KuCoin so the assets were no longer associated with the original/stolen assets or traceable on the ledger. For numerous years after the launch of KuCoin's crypto exchange, the KuCoin Crypto-Wash Enterprise became a leading conduit of cryptocurrency stolen from U.S. citizens, residents, and entities, enabling bad actors to seamlessly transfer stolen crypto around the United States and the world.

7. KuCoin knew, or should have known, that certain KuCoin customer wallet addresses were associated with prior illicit activity and were blacklisted. Instead of closing those accounts,

freezing the assets in those accounts, or reporting the accounts to the authorities, KuCoin kept them open and allowed bad actors to continue using those same KuCoin accounts to launder crypto.

8. Eventually, the authorities caught up with the KuCoin Defendants. It was not until the KuCoin Defendants were notified of a federal criminal investigation into their activities in July 2023 that KuCoin purportedly implemented a KYC program requiring verification of user identities. These measures, however, applied to new customers only and, at that time, did not apply to KuCoin's millions of existing customers, including the substantial number of customers based in the United States.

9. On December 12, 2023, defendants Mek Global and PhoenixFin reached a settlement with the state of New York in connection with the New York Attorney General's ("NYAG") March 9, 2023 lawsuit against KuCoin. As part of the settlement, KuCoin paid ***more than $22 million*** in refunds and penalties. KuCoin also admitted to, among other things, operating as an unregistered securities or commodities broker-dealer and exchange.

10. In March 2024, an indictment was unsealed by the U.S. Department of Justice ("DOJ") and the U.S. Department of Homeland Security ("DHS") for the scheme alleged herein against defendants Flashdot, Peken Global, and PhoenixFin, and defendants Gan and Tang. The Commodity Futures Trading Commission ("CFTC") also filed a civil enforcement action charging Mek Global, PhoenixFin, Flashdot, and Peken Global for violations of federal laws and regulations.

11. In January 2025, in response to the DOJ's indictment, defendant Peken Global pled guilty to operating an unlicensed MTB, and agreed to, *inter alia*, pay to the U.S. government monetary penalties totaling ***more than $297 million***. Similarly, defendants Gan and Tang each agreed to forfeit to the U.S. government ***$2.7 million in ill-gotten gains*** and to forgo any future role in KuCoin's operations or management. The CFTC action is ongoing as of the date of this filing.

12. Plaintiffs bring claims on behalf of themselves and all other persons or entities in the United States whose cryptocurrency was removed from a digital wallet, account, or protocol as a result of a hack, ransomware attack, or theft and, between August 21, 2020 and the date of Judgment (the "Class Period"), was transferred to a KuCoin account, and who have not recovered some, or all, of their cryptocurrency that was transferred to KuCoin (the "Class").

13. Plaintiffs allege claims for violations of the Racketeer Influenced and Corrupt Organizations ("RICO") Act, 18 U.S.C. §§1962(c)-(d), conversion, and aiding and abetting conversion.

14. In asserting the claims herein, Plaintiffs are not relying on any contracts or agreements entered into between KuCoin and any users of KuCoin to assert any claims alleged herein, and none of Plaintiffs' claims derive from the underlying terms of any such contracts or agreements. Plaintiffs are not relying on any actions Defendants have taken or could have taken, or benefits Defendants have received or could have received, pursuant to the terms of any contracts or agreements with users of KuCoin. Rather, Plaintiffs' claims are based on Defendants violating federal statutory obligations and engaging in the conversion of, and aiding and abetting the conversion of, cryptocurrency properly belonging to Plaintiffs and members of the Class.

15. Specifically, Defendants, *inter alia*: (i) committed, and aided and abetted, acts constituting indictable offenses under 18 U.S.C. §1960 (relating to illegal money transmitters) and 18 U.S.C. §1961(1)(E) (act indictable under the Currency and Foreign Transactions Reporting Act a/k/a the BSA); and (ii) aided and abetted acts constituting indictable offenses under 18 U.S.C. §1956 (laundering of monetary instruments), 18 U.S.C. §1957 (engaging in monetary transactions in property derived from specified unlawful activity), and 18 U.S.C. §2314 (relating to interstate transportation of stolen property).

16. Plaintiffs seek damages and equitable relief on behalf of themselves and the putative Class, including, but not limited to: treble their monetary damages; injunctive relief; damages; costs and expenses, including attorneys' and experts' fees; interest; and any additional relief that this Court determines to be necessary or appropriate to provide complete relief to Plaintiffs and the Class.

JURISDICTION AND VENUE

17. This Court has original jurisdiction over the subject matter of this action pursuant to 28 U.S.C. §1331, because Plaintiffs' claims arise under the RICO Act, 18 U.S.C. §1962. The RICO Act provides for nationwide service of process, and Defendants conduct a substantial portion of their business in the United States. This Court has personal jurisdiction over Defendants pursuant to 18 U.S.C. §§1965(b) and (d).

18. The Court also has jurisdiction over this action pursuant to 28 U.S.C. §1332(d), because the members of the putative Class are of diverse citizenship from Defendants, there are more than 100 members of the putative Class, and the aggregate amount in controversy exceeds $5,000,000, exclusive of costs and interest.

19. The Court has specific personal jurisdiction over Defendants because they: (i) transact business in New York; (ii) have substantial aggregate contacts with New York; (iii) engaged in conduct that had a direct, substantial, and reasonably foreseeable and intended effect of causing injury to persons in New York; and (iv) purposely availed themselves of the laws of New York. Among other things, the KuCoin Defendants operated the KuCoin cryptocurrency exchange in New York, serviced New York customers, and refused to comply with the BSA and implement required KYC and AML policies in New York. This Court also has specific personal jurisdiction over the KuCoin Defendants for the additional reason that they asserted substantial control over KuCoin and

its crypto exchange, as described below. Additionally, defendant Chainalysis' headquarters is located in New York, New York.

20. Exercising jurisdiction over Defendants in this forum is reasonable and comports with fair play and substantial justice.

21. Venue is proper in this District pursuant to 28 U.S.C. §1391 because the KuCoin Defendants, as foreign entities and individuals, may be sued in any judicial district. *See* 28 U.S.C. §1391(c)(3). Venue is similarly proper for defendant Chainalysis, which maintains its corporate headquarters in New York, New York. *See* 28 U.S.C. §1391(c)(2).

PARTIES

Plaintiffs

22. Plaintiff Sofia Reca is an individual domiciled in Surfside, Florida. In May 2021, while plaintiff Reca resided in the U.S., an unknown third party targeted plaintiff Reca's Atomic Wallet account located in the U.S. and stole from her ten different cryptocurrencies (then valued at approximately $1,400,000.00 USD). After an extensive investigation, it was determined that, between May 2021 and July 2021, a material portion of the cryptocurrency stolen from plaintiff Reca was sent to at least one account at KuCoin. At no time has plaintiff Reca ever held an account with KuCoin or ever agreed to any terms of use that KuCoin imposes upon its accountholders.

23. Plaintiff James K. Supples is an individual domiciled in San Juan, Puerto Rico. In December 2024, while plaintiff Supples resided in a U.S. territory, unknown hackers targeted plaintiff Supples' MEXC.com account located in the U.S. and stole from him six different cryptocurrencies (then valued at approximately $1,200,000.00 USD). After an extensive investigation, it was determined that, in December 2024, a material portion of the cryptocurrency stolen from plaintiff Supples was sent to at least one account at KuCoin. Each of the Plaintiffs

referenced in ¶¶22-23 reside in the U.S. (or its territories) and had their cryptocurrency stolen from them in the U.S.

24. Upon information and belief, KuCoin's exchange, where the cryptocurrency stolen from Plaintiffs was laundered, was housed on U.S. servers.

25. Upon information and belief, KuCoin failed to apply KYC and AML procedures, as required by statutory law, to detect the lawful ownership of the cryptocurrency properly belonging to Plaintiffs or members of the Class.

Defendants

26. Defendant Flashdot Limited f/k/a PhoenixFin Limited ("Flashdot") is a company incorporated in the Cayman Islands and, during much of the Class Period, was the holding company of the KuCoin cryptocurrency exchange.

27. Defendant Mek Global Limited ("Mek Global") is incorporated under the laws of the Republic of Seychelles. At times during the Class Period, KuCoin operated under the legal name Mek Global Limited. According to the NYAG Consent Order (defined below), Mek Global is no longer an owner of the KuCoin cryptocurrency trading platform.

28. Defendant Peken Global Limited ("Peken Global"), an entity located at Room 306, Victoria House, Victoria Mahe, Seychelles, has operated KuCoin since in or about September 2019. According to the NYAG Consent Order, Peken Global is the current owner of the KuCoin cryptocurrency trading platform. Defendant Peken Global is controlled by defendants Gan and Tang, who are its sole shareholders, and defendant Gan is Peken Global's Director.

29. Defendant PhoenixFin Private Limited ("PhoenixFin") is incorporated under the laws of Singapore and operated KuCoin from about September 2017 through in or about December 2018. As of in or about May 2018, defendant Gan was the Chief Executive Officer ("CEO") of PhoenixFin, and defendant Tang was its President. According to the CFTC Complaint (defined

below), from at least July 2019 until at least June 2023, PhoenixFin was the owner of the "KuCoin.com" domain.

30. Defendants Flashdot, Mek Global, Peken Global, and PhoenixFin have operated the KuCoin cryptocurrency trading platform since at least 2017. They share the same founding team, management team, and operation team. They advertise on a single website, which does not distinguish between entities. Employees of these entities have "@kucoin.com" email addresses. At all times relevant herein these entities operated as an integrated, common enterprise, and are collectively referred to herein as "KuCoin." KuCoin has never had a physical presence in either the Seychelles or the Cayman Islands, where certain of the Defendants are incorporated. KuCoin's employees and physical operations are located in Singapore and China, among other places.

31. Defendant Chun (a/k/a "Michael") Gan ("Gan") co-founded KuCoin with defendant Tang and others, and along with defendant Tang, owns approximately 75% of the shares in Flashdot.

32. Defendant Ke (a/k/a "Eric") Tang ("Tang") co-founded KuCoin with defendant Gan and others, and along with defendant Gan, owns approximately 75% of the shares in Flashdot.

33. Defendants Gan and Tang are collectively referred to herein as the "Individual Defendants." At all times relevant herein, until they were required to step down from their roles at KuCoin as a result of a deferred prosecution agreement with the DOJ, the Individual Defendants operated, managed, and controlled KuCoin and its operations, including through their ownership and control in one or more of the entities comprising KuCoin, including defendants Flashdot, Mek Global, Peken Global, and PhoenixFin. The Individual Defendants reaped substantial financial benefits from their operation and control of KuCoin, including as a result of fees and revenues generated by the KuCoin Crypto-Wash Enterprise.

34. Defendant Chainalysis, Inc. ("Chainalysis"), a Delaware corporation headquartered in New York, New York, is a crypto-tracing analysis company that was retained by KuCoin throughout the Class Period to implement software solutions to identify, analyze, and track cryptocurrency and transactions. Chainalysis also offered to its customers "insightful user analytics for strategic user retention and growth." Among other things, KuCoin used Chainalysis' proprietary Know-Your-Transaction ("KYT") software, which was designed to identify and purportedly block money laundering and other illicit actions in real-time. Chainalysis also provided its proprietary "Reactor" software for KuCoin to investigate suspicious activities. KuCoin characterized its dealings with Chainalysis as a partnership to purportedly deepen KuCoin's commitment to security and compliance, but those statements were for appearances only. Even though Chainalysis enabled KuCoin to have access to information about illicit transactions, KuCoin refused to take any steps to prevent them. Chainalysis reaped substantial financial benefits from its partnership with KuCoin, including as a result of fees and revenues generated by the KuCoin Crypto-Wash Enterprise.

COMMON FACTUAL ALLEGATIONS

KuCoin and Its Business

35. Defendants Gan, Tang, and others founded KuCoin in or about September 2017, and Gan and Tang have been co-owners of KuCoin since its founding. From its inception, KuCoin has been owned and operated by and through one or more companies, including defendants Flashdot, Peken Global, and PhoenixFin. According to the DOJ Indictment (defined below), as of March 2022, Gan and Tang have been directors of Flashdot and together held approximately 75% of the shares in Flashdot. Peken Global and PhoenixFin are subsidiaries and/or affiliates of Flashdot.

36. KuCoin's employees and physical operations are located in Singapore and China, among other places. KuCoin never had a physical presence in either Seychelles or the Cayman Islands.

37. During the Class Period, KuCoin claimed to allow customers to "Trade Anytime, Anywhere." In furtherance of this goal, KuCoin's KYC procedures were either non-existent or a sham, and U.S. customers were able to use KuCoin's platform to trade cryptocurrency.

38. Customers in the United States could create a KuCoin account with only an email address or telephone number and engage in financial transactions without providing any proof of identity. Furthermore, any purported written policies against serving U.S.-based customers were for appearances only, as KuCoin did not even attempt to block U.S. customers based on their internet protocol ("IP") address location.

Overview of Defendants' Scheme and the KuCoin Crypto-Wash Enterprise

39. KuCoin launched its cryptocurrency exchange at KuCoin.com in September 2017, where it enabled customers to open accounts and engage in cryptocurrency transactions. When a user opened an account, KuCoin assigned them a custodial virtual currency wallet – *i.e.*, a wallet in KuCoin's custody, which enabled the user to conduct various types of transactions on the platform, such as swapping one crypto for another, transferring funds to other KuCoin accounts, withdrawing crypto out of KuCoin, sending the crypto to external virtual currency wallets, or converting the crypto to fiat currency and transferring it to bank accounts.

40. KuCoin charges fees to customers for engaging in crypto transactions, so the more transactions customers completed, the more KuCoin earned. KuCoin has a strong monetary incentive to encourage, facilitate, and allow as many transactions on its exchange as possible – even transactions involving stolen cryptocurrency.

41. KuCoin solicited and accepted orders, accepted property to margin, and operated a facility for trading futures, swaps, and leveraged, margined, or financed retail transactions involving digital assets that are commodities, including BTC, ETH, and Litecoin.

42. From its founding in September 2017 until at least December 2023, KuCoin served, and actively sought to serve, customers located in the United States, including within the Southern District of New York. Moreover, U.S.-based customers were a critical part of KuCoin's growth strategy, such that during the Class Period, between 20% and 50% of KuCoin's users were located in the United States.

43. Since KuCoin conducted a substantial portion of its business in the United States, its practice of permitting users to open accounts, conduct transactions, and withdraw cryptocurrency without providing identification violated U.S. laws and regulations. Defendants knew KuCoin was required to, but failed to, implement KYC and AML procedures. Defendants willfully violated these important U.S. laws and regulations to maximize fees and gain market share. KuCoin's failure to implement an effective AML program along with Defendants' prioritization of growth, market share, and profits over compliance with U.S. law enabled KuCoin to rapidly become one of the largest cryptocurrency exchanges in the world.

44. According to an August 30, 2021 KuCoin press release, from its founding to that date, KuCoin had executed 810 million transactions and had accumulated transaction volume valued at $400 billion. From August 2020 to August 2021, the average daily trading volume had grown by 791% and was $4.3 billion as of August 31, 2021. By December 8, 2021, KuCoin reached ten million registered users, which according to a KuCoin December 8, 2021 press release, caused KuCoin to become one of the five largest cryptocurrency exchanges in the world. According to the same press release, "KuCoin experienced a 9-fold increase in newly registered users compared to the previous year, and 23 times year-over-year growth in trading volumes."

45. KuCoin continued to experience strong growth during 2022 and 2023. It added over 9.75 million new registered users in the first half of 2022 and reached a total user base of over 20

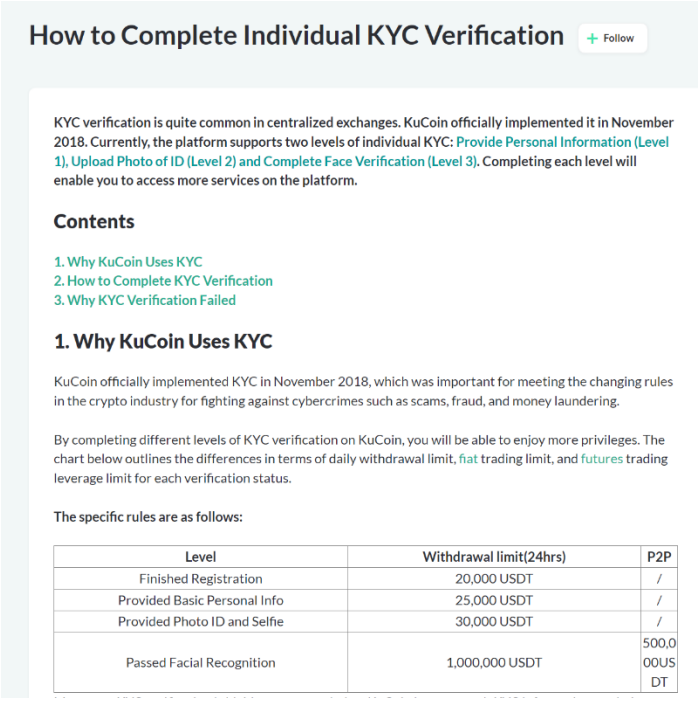
million users, resulting in a doubling of users from 10 million users in December 2021 to 20 million users only 7 months later. According to a June 28, 2023 KuCoin press release, by June 2023, KuCoin had 27 million users in 207 countries and regions and offered over 700 digital assets. According to KuCoin's website as of June 2024, KuCoin has 30 million registered users, and it was ranked as the fifth-largest cryptocurrency exchange in terms of overall performance by CoinMarketCap.com and Coingecko.com.

46. The amount of fees KuCoin charged a user varied based on the user's trading volume, as higher-volume traders typically paid lower fees per trade. Higher-volume traders also helped provide liquidity on KuCoin's platform. Generating a large number of trades and maintaining high liquidity is very important for a crypto exchange. A highly liquid market is generally more desirable from the end-user's standpoint because the bid and ask spreads will typically be narrower and larger trades can be conducted more easily. A highly liquid exchange, however, also makes it easier for bad actors to exchange large amounts of stolen crypto.

47. KuCoin created several levels of user accounts based on the amount of self-identifying information a customer provided as well as whether a customer was an individual or an institution. Beginning from KuCoin's launch in 2017 until at least July 14, 2023, KuCoin enabled customers to open accounts and trade crypto ***without providing KYC information***. KuCoin's website described the most basic level of membership as the "Finished Registration" level in 2021 and the "Unverified" level in 2022 (collectively, "Level 1" users). A user could open an account in the "Unverified" or "Finished Registration" level with an email and password and without providing KYC information. During 2021, as long as a user was in the "Finished Registration" level, they could withdraw up to $20,000 per day, and if someone was in the "Unverified" level in 2022, they could withdraw up to one BTC per day. The price of BTC traded over $40,000 in 2022 and 2023, so

"Unverified" level users could withdraw a considerable amount of funds from each account every 24 hours.

48. Below is a screenshot from KuCoin's website on or about June 4, 2021:



How to Complete Individual KYC Verification + Follow

KYC verification is quite common in centralized exchanges. KuCoin officially implemented it in November 2018. Currently, the platform supports two levels of individual KYC: Provide Personal Information (Level 1), Upload Photo of ID (Level 2) and Complete Face Verification (Level 3). Completing each level will enable you to access more services on the platform.

Contents

1. Why KuCoin Uses KYC
2. How to Complete KYC Verification
3. Why KYC Verification Failed

1. Why KuCoin Uses KYC

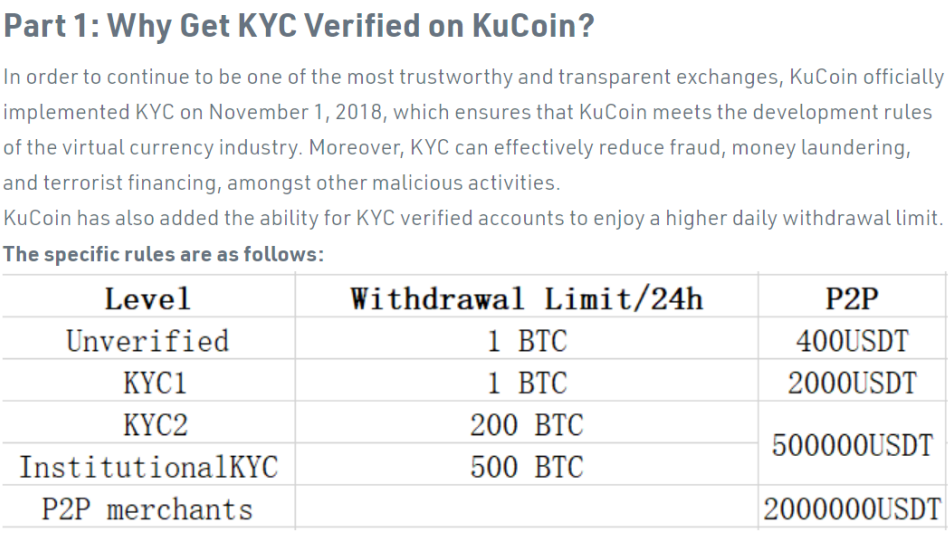
KuCoin officially implemented KYC in November 2018, which was important for meeting the changing rules in the crypto industry for fighting against cybercrimes such as scams, fraud, and money laundering.

By completing different levels of KYC verification on KuCoin, you will be able to enjoy more privileges. The chart below outlines the differences in terms of daily withdrawal limit, fiat trading limit, and futures trading leverage limit for each verification status.

The specific rules are as follows:

Level	Withdrawal limit(24hrs)	P2P
Finished Registration	20,000 USDT	/
Provided Basic Personal Info	25,000 USDT	/
Provided Photo ID and Selfie	30,000 USDT	/
Passed Facial Recognition	1,000,000 USDT	500,000USDT

49. Below is a screenshot from KuCoin's website on or about November 28, 2022:



Part 1: Why Get KYC Verified on KuCoin?

In order to continue to be one of the most trustworthy and transparent exchanges, KuCoin officially implemented KYC on November 1, 2018, which ensures that KuCoin meets the development rules of the virtual currency industry. Moreover, KYC can effectively reduce fraud, money laundering, and terrorist financing, amongst other malicious activities.

KuCoin has also added the ability for KYC verified accounts to enjoy a higher daily withdrawal limit.

The specific rules are as follows:

Level	Withdrawal Limit/24h	P2P
Unverified	1 BTC	400USDT
KYC1	1 BTC	2000USDT
KYC2	200 BTC	500000USDT
InstitutionalKYC	500 BTC	
P2P merchants		2000000USDT

50. While Level 1 users had certain withdrawal limitations, KuCoin did not restrict the amount of crypto a user could transfer into KuCoin or trade at KuCoin based on level. Additionally, KuCoin allowed Level 1 users to open multiple accounts by providing a new email address for each account, which effectively circumvented the withdrawal limit.

51. Even though KuCoin enabled users to open accounts and fully use KuCoin's exchange without providing any KYC information, KuCoin professed to have implemented KYC verification because it offered account levels with larger withdrawal limits if users provided self-identifying information. For example, KuCoin falsely represented on its website in 2021 and 2022 that it officially implemented KYC verification on November 1, 2018. This was false, and KuCoin did not implement KYC policies and procedures in compliance with U.S. laws and regulations because it continued to offer users an account level that did not require any KYC information. KuCoin's offer of increased withdrawal limits in exchange for users voluntarily providing self-identifying information did not comply with KYC and AML rules and regulations.

52. Even though KuCoin acknowledged on its website that "KYC can effectively reduce fraud, money laundering, and terrorist financing, amongst other malicious activities," KuCoin willfully refused to implement KYC requirements to prevent bad actors from laundering crypto at KuCoin. Since KuCoin continued offering users the ability to utilize KuCoin without providing KYC information, KuCoin knowingly permitted bad actors to freely open accounts and launder crypto through their KuCoin accounts.

53. KuCoin knew, or should have known, that numerous KuCoin customer wallet addresses were associated with prior illicit activity and were blacklisted. During the Class Period, the KuCoin Defendants had access to tools, platforms, and crypto-tracing analysis services, including from partner/defendant Chainalysis, that enabled them to easily identify whether crypto

was transferred from an external wallet or to a KuCoin account that had previously been identified as being associated with illicit activity. According to a March 11, 2022 article on CoinDesk.com titled "How Authorities Track Criminal Crypto Transactions," blockchain analytic firms like defendant Chainalysis have created tools that identify wallets associated with illicit activities and that "it is possible to ascertain how many wallets a criminal controls from a single transaction that might've occurred after a hack, rug pull or any type of unlawful cyber activity was perpetrated."

54. KuCoin permitted numerous blacklisted KuCoin deposit addresses to continue transacting on the KuCoin platform. KuCoin, as a member of the Crypto Defender's Alliance ("CDA") throughout the Class Period, an invite-only group of approximately 360 members, including exchanges, swap protocols, forensic companies, and verified investigators, had access to the blacklist, yet permitted these deposit accounts to continue using the KuCoin platform. In many instances, blacklisted KuCoin deposit addresses were able to continue to transact on the KuCoin platform years after the date of blacklisting.

55. Instead of closing those accounts, freezing their assets, or reporting them to the authorities, KuCoin kept them open and allowed bad actors to continue using those same KuCoin accounts to launder crypto. For example, even though a KuCoin deposit address was blacklisted on or about July 13, 2022, that same address received additional deposits during September 2023 and February 2024. Other examples include, but are not limited to, the following:

(a) a KuCoin wallet was blacklisted on or about March 15, 2024, but that same wallet received additional deposits from March to April 2025;

(b) a KuCoin wallet was blacklisted on or about March 23, 2024, but that same wallet received additional deposits in December 2024 and January 2025;

(c) a KuCoin wallet was blacklisted on or about May 4, 2024, but that same wallet received additional deposits in July 2024;

(d) a KuCoin wallet was blacklisted on or about October 17, 2023, but that same wallet received additional deposits in January, February and May of 2024; and

(e) a KuCoin wallet was blacklisted on or about June 24, 2022, but that same wallet received additional deposits in June and July of 2022.

56. In fact, KuCoin permitted a KuCoin deposit account to receive more than 20,000 transfers valued at more than $2,300,000 after it was blacklisted.

KuCoin Was, and Is, Subject to Important U.S. Laws and Regulations

57. Once KuCoin began conducting business in the United States, it became subject to strict regulations aimed at, among other things, creating a protocol for identifying suspicious activity that might indicate potential money laundering operations and other illegitimate activities by its customers. In addition, KuCoin was required to have procedures in place for reporting illicit activities to relevant authorities.

58. Specifically, due to the nature of KuCoin's business and services offered to customers, KuCoin was an MTB required to register with the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") and, since in or about July 2019, when KuCoin launched a derivatives trading platform, it has been a futures commission merchant ("FCM"). As a result, KuCoin was required to comply with the provisions of the BSA, 31 U.S.C. §5311 *et seq*., applicable to MTBs and FCMs.

59. The Currency and Foreign Transactions Reporting Act, its amendments, and the other statutes relating to the subject matter of that Act have come to be referred to as the BSA. These statutes are codified at 12 U.S.C. §1829b, 12 U.S.C. §§1951-1959, 18 U.S.C. §1956, 18 U.S.C. §1957, 18 U.S.C. §1960, and 31 U.S.C. §§5311-5314 and 5316-5332 and notes thereto.

60. The BSA, as amended by the USA PATRIOT ACT of 2001, is designed to "prevent the laundering of money and the financing of terrorism" and "protect the financial system of the United States from criminal abuse." 31 U.S.C. §5311. The BSA imposes reporting, recordkeeping, and controls requirements on covered "financial institutions," which include FCMs that are required to register as such under the Commodity Exchange Act ("CEA"), and MTBs "who engage[] as a business in the transmission of currency, funds, or value that substitutes for currency" and are required to register as such with FinCEN. 31 U.S.C. §5312.

61. The CEA requires an entity to register as an FCM with the CFTC if it solicits or accepts orders for commodity futures contracts, swaps, or retail commodity transactions (among other specified products), and in or in connection with such activity accepts any money or property to margin, guarantee, or secure any trades or contracts that result or may result therefrom. Bitcoin and other cryptocurrency are "commodities" under the CEA.

62. Under the BSA, an FCM must establish an AML program that is approved by senior management and that includes, at a minimum: "[P]olicies, procedures, and internal controls reasonably designed to prevent the financial institution from being used for money laundering or the financing of terrorist activities"; independent compliance testing; ongoing training for appropriate personnel; and "risk-based procedures for conducting ongoing customer due diligence." *See* 31 U.S.C. §5318(h)(l); 31 C.F.R. §1026.210. FCMs must also file suspicious activity reports ("SARs") in certain situations, including when a transaction involves funds or other assets of at least $5,000 and the FCM knows, suspects, or has reason to suspect that the transaction involves funds derived from illegal activity or that the FCM is being used to facilitate criminal activity. *See* 31 C.F.R. §1026.320.

63. As part of its AML program, an FCM must implement a written KYC program that includes "risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable." This KYC program must enable an FCM to "form a reasonable belief that it knows the true identity of each customer." At a minimum, an FCM must collect the name, date of birth, address, and government identification number of each customer prior to account opening, and must take steps to verify that information in a reasonable time. The KYC program must also include procedures for "determining whether a customer appears on any list of known or suspected terrorists or terrorist organizations issued by any Federal government agency." *See* 31 U.S.C. §5318(1); 31 C.F.R. §1026.220.

64. The BSA also requires MTBs to register with the U.S. Secretary of the Treasury. *See* 31 U.S.C. §5330. Cryptocurrency exchanges that accept and transmit cryptocurrencies are MTBs. Under the BSA and its implementing regulations, MTBs must "develop, implement, and maintain an effective anti-money laundering program," *i.e.*, "one that is reasonably designed to prevent the money services business from being used to facilitate money laundering and the financing of terrorist activities." 31 C.F.R. §1022.210. At a minimum, an effective AML program must include customer identification procedures, a compliance officer, training and education of appropriate personnel in the AML program, and provide for independent review to monitor and maintain an adequate program. *See id*. MTBs must also identify and report suspicious transactions relevant to a possible violation of law or regulations with the U.S. Department of the Treasury. *See* 31 C.F.R. §1022.320.

65. The Bank Secrecy Act/Anti-Money Laundering Examination Manual promulgated by the Federal Financial Institutions Examination Council ("FFIEC Manual") also summarizes industry sound practices and examination procedures for customer due diligence on accounts that present a

higher risk for money laundering and terrorist financing. The FFIEC Manual sets forth a matrix for identifying high risk accounts that require enhanced due diligence. Such accounts include those that have "large and growing customer[s] base[d] in a wide and diverse geographic area" or "[a] large number of noncustomer funds transfer transactions and payable upon proper identification . . . transactions" and "[f]requent funds from personal or business accounts to or from higher-risk jurisdictions, and financial secrecy havens or jurisdictions," such as KuCoin's deposit accounts.

66. KuCoin was required to comply with heightened due diligence for its deposit accounts. According to the FFIEC Manual, KuCoin's due diligence was required to include assessments to determine the purpose of the account, ascertain the source and funding of the capital, identify account control persons and signatories, scrutinize the account holders' business operations, and obtain adequate explanations for account activities.

67. KuCoin's general customer due diligence program was required to include protocols to predict the types of transactions, dollar volume, and transaction volume each customer is likely to conduct, and furnish a means for KuCoin to notice unusual or suspicious transactions for each customer.

68. Furthermore, KuCoin's customer due diligence process must be able to identify any of a series of money laundering "red flags" as set forth in the FFIEC Manual, including: (i) frequent involvement of multiple jurisdictions or beneficiaries located in higher-risk offshore financial centers; (ii) repetitive or unusual funds transfer activity; (iii) funds transfers sent or received from the same person to or from different accounts; (iv) unusual funds transfers that occur among related accounts or among accounts that involve the same or related principals; (v) transactions inconsistent with the account holder's business; (vi) customer use of a personal account for business purposes; (vii) multiple accounts established in various corporate names that lack sufficient business purpose

to justify the account complexities; and (viii) multiple high-value payments or transfers between shell companies without a legitimate business purpose. The due diligence process must also enable KuCoin to take appropriate action once such "red flags" are identified.

69. As alleged herein, Defendants willfully and flagrantly ignored these important U.S. rules and regulations, which enabled KuCoin to become a central hub of crypto trading for bad actors, including those who sought to utilize the KuCoin Crypto-Wash Enterprise.

KuCoin's Partnership with Chainalysis

70. On June 1, 2020, KuCoin announced a partnership with Chainalysis to "further deepen KuCoin's commitment to security and compliance." KuCoin went on to state that "[t]he exchange will use Chainalysis' Know-Your-Transaction (KYT) software to expose and block money laundering and other illicit actions in real-time[.] . . . In addition, Chainalysis Reactor will be used for conducting further investigations into suspicious activities." KuCoin further stated that Chainalysis Reactor "aids in identifying and stopping bad actors, which use cryptocurrency for illegal activities like money laundering, fraud, and extortion."

71. The announcement further stated:

> Through Chainalysis KYT, compliance departments can monitor cryptocurrency actions and detect high-risk transactions by using AML standards to each transaction across every user in an organization.

72. KuCoin proclaimed that "[w]ith this collaboration, the two companies will continue to promote compliance-first business practices in the crypto world."

73. KuCoin Global CEO, Johnny Lyu, commented on the partnership by stating:

> We teamed up with Chainalysis to create a safe and compliant trading environment. Through KuCoin's efforts, the crypto world will combat illegal activities, such as laundering money and financing terrorism. Although KuCoin has already deployed in this aspect, we hope to further strengthen our technical expansion into compliance with our cooperation with Chainalysis. Not only does it provide infrastructure to the blockchain ecosystem, but it also meets regulatory compliance requirements across different countries and regions.

74. Chainalysis' Chief Revenue Officer Jason Bonds also made the following remarks:

> Chainalysis is thrilled to partner with exchanges like KuCoin that prioritize compliance and the safety of its users. Our relationship with KuCoin is also an example of our continued commitment to working with leading exchanges in the Asia Pacific region, an important hub of cryptocurrency activity.

75. A few months later, on September 25, 2020, Chainalysis demonstrated its crypto-tracing expertise by helping KuCoin and government authorities identify "hackers [who] stole more than $275 million worth of cryptocurrency from KuCoin in one of the largest ever exchange hacks." Chainalysis attributed this success to its proprietary software Reactor, which allowed its team of investigators to trace these funds despite several "complicating effects" involving decentralized exchanges where "users can complete these currency swaps without having to provide KYC (know-your-customer) information or the trades being recorded in an order book as they would be on a standard cryptocurrency exchange."

76. Based on these representations and results, Chainalysis had the resources and expertise to help KuCoin identify bad actors who laundered cryptocurrency obtained through hacks, ransomware attacks, and theft and thereafter launder through KuCoin.

77. The partnership between Chainalysis and KuCoin benefitted both entities and furthered the scheme alleged herein. Their partnership enabled Chainalysis to earn lucrative fees and gain widespread media coverage, and enabled KuCoin to make it appear as if it were seeking to comply with KYC and AML rules and regulations, even though that was not true.

78. Even though Chainalysis provided KuCoin with software and informational alerts to prevent bad actors from laundering crypto at the KuCoin exchange, the KuCoin Defendants refused to implement the policies or procedures necessary to stop or catch the bad actors. Indeed, although KuCoin and Chainalysis may have assisted in the identification of the crypto stolen by the hackers as described above, that was a very rare exception to KuCoin's normal practices. KuCoin highlighted

its partnership with Chainalysis to make it appear as though KuCoin was committed to complying with the law when Defendants knew that was not true. In reality, as both the KuCoin Defendants and Chainalysis were aware, even though KuCoin had access to information and red flags alerting KuCoin to potential crypto laundering and other illicit activities, KuCoin refused to implement adequate KYC and AML policies and procedures or dedicate resources to attempt to prevent those activities. They also knew that KuCoin was a magnet and hub for bad actors to launder cryptocurrency. Chainalysis was complicit with the KuCoin Defendants' refusal to prevent money laundering on the KuCoin platform in order to maintain the benefits of its partnership with KuCoin.

AML and KYC Laws and Regulations Are Intended to Catch Criminals and Protect Innocent Consumers Like Plaintiffs

79. The BSA, the USA PATRIOT Act, and related AML/KYC regulations were enacted to combat money laundering and terrorist financing. These laws and regulations protect consumers by aiding government officials and law enforcement in efforts to stop, or identify the culprits of, illicit transactions.

80. Pursuant to the USA PATRIOT Act, KuCoin was required to implement KYC programs to identify its customers. These KYC regulations exist to, among other reasons, prevent known bad actors from engaging in illicit financial transactions.

81. Many of the wallets used by bad actors to steal and launder funds are designated as "blacklisted wallets," meaning they are flagged by authorities or exchanges as being involved in illegal or fraudulent activities. Exchanges like KuCoin have access to lists of blacklisted wallets and are expected to block those wallets from sending or receiving transactions. The failure to block these wallets enables further illicit activity.

82. Moreover, MTBs, like KuCoin, must file a SAR whenever they uncover information that raises suspicion of, *inter alia*, insider activity, money laundering, terrorist financing, and other criminal activity. SARs are archived for five years after they are filed.

83. KuCoin was required, pursuant to the BSA, to file a SAR within 30 to 60 calendar days of detecting each of the suspicious transactions involving Plaintiffs' and Class members' stolen assets.

84. U.S. governmental entities and law enforcement rely on SARs to detect patterns and trends in organized and personal financial crimes. This allows law enforcement to anticipate and counteract criminal and fraudulent behavior.

85. Victims of financial crimes, such as Plaintiffs and the members of the Class, are beneficiaries of the rules and regulations governing KYC and AML policies and procedures, including those in the BSA and the USA PATRIOT Act. These rules exist to prevent known or suspicious bad actors from opening and maintaining accounts at financial institutions and to enable the victims of financial crimes to track their stolen assets and identify the culprits.

86. Because applicable laws require MTBs to implement and maintain AML and KYC policies and procedures, it was reasonably foreseeable that KuCoin's failure to implement and maintain adequate AML and KYC policies and procedures would cause bad actors to launder stolen cryptocurrency through KuCoin.com.

87. Had the KuCoin Defendants complied with applicable laws and regulations, including, but not limited to, the BSA, KuCoin would not have become a magnet and hub for cryptocurrency laundering; and it is highly unlikely that Plaintiffs' and Class members' stolen cryptocurrency would have been laundered through KuCoin.com and rendered untraceable thereafter.

The KuCoin Defendants Were Charged with, and Pled Guilty to, Violating U.S. Laws and Regulations

The KuCoin Defendants Paid Over $300 Million to Settle Charges Filed by the DOJ

88. On January 27, 2025, defendant Peken Global pled guilty to charges, filed by the DOJ, of operating an unlicensed MTB in violation of 18 U.S.C. §1960 and 18 U.S.C. §2. In addition to the guilty plea, defendant Peken Global agreed to criminally forfeit to the U.S. government $184.5 million and pay a criminal fine of approximately $112.9 million, for a total of approximately $297 million. Defendant Peken Global further agreed that KuCoin would not conduct business in the U.S. for at least the next two years.

89. Additionally, on January 27, 2025, pursuant to the Speedy Trial Act, the DOJ and defendants Gan and Tang agreed to defer the prosecution of defendants Gan and Tang for two years. As part of the agreement, defendants Gan and Tang agreed to each forfeit to the U.S. government over $2.7 million in ill-gotten gains.

90. Defendants Gan and Tang, as part of their agreement with the DOJ, also admitted that they "knowingly owned, from at least in or about September 2017 through at least in or about December 2023, part of a money transmitting business that was not registered or licensed in the United States." Additionally, defendants Gan and Tang agreed that their "conduct, as admitted, violated Title 18, United States Code, Sections 1960(a) and (b)(1)(A) and (B)." Finally, defendants Gan and Tang agreed to forgo any future involvement in the management or operation of KuCoin.

91. On January 27, 2025, at the plea and sentencing hearing, defendant Peken Global admitted to the following:

> Since its launch, ***KuCoin has served approximately 1.5 million registered users located in the United States***, including registered users located in the Southern District of New York. Because KuCoin had a significant number of . . . registered users located in the United States, KuCoin knowingly conducted a money transmitting business that was required to register with the U.S. Department of the Treasury's Financial Crimes Enforcement Network, known as FinCEN. KuCoin

> violated United States law by failing to register with FinCEN as a money transmitting business[.]

92. Defendant Peken Global also acknowledged that it "knowingly" engaged in such conduct, and "that the conduct affected interstate and foreign commerce."

93. In a press release from the U.S. Attorney's Office for the Southern District of New York, U.S. Attorney Danielle R. Sassoon stated:

> For years, KuCoin avoided implementing required anti-money laundering policies designed to identify criminal actors and prevent illicit transactions. As a result, ***KuCoin was used to facilitate billions of dollars' worth of suspicious transactions and to transmit potentially criminal proceeds***, including proceeds from darknet markets and malware, ransomware, and fraud schemes. Today's guilty plea and penalties show the cost of refusing to follow these laws and allowing unlawful activity to continue.

94. According to the DOJ, "KuCoin employees repeatedly stated on public social media sites that ***KYC was not mandatory*** on KuCoin, including in response to posts from customers who had identified themselves as being in the U.S."

95. Moreover, according to the DOJ, "KuCoin also never registered with FinCEN as a money transmitting business or filed any required suspicious activity reports. As a result of KuCoin's failure to maintain the required AML and KYC programs, KuCoin was used to transmit billions in suspicious transactions and potentially criminal proceeds, including proceeds from darknet markets and malware, ransomware, and fraud schemes."

96. KuCoin, including defendants Flashdot, Peken Global, and PhoenixFin, and defendants Gan and Tang, were originally indicted by the U.S. Attorney for the Southern District of New York and the Acting Special Agent in Charge of the New York Field Office of Homeland Security Investigations ("HSI") for: (i) conspiring to operate an unlicensed MTB and conspiring to violate the BSA by willfully failing to maintain an adequate AML program designed to prevent KuCoin from being used for money laundering and terrorist financing; (ii) failing to maintain

reasonable procedures for verifying the identity of customers; and (iii) failing to file any suspicious activity reports. KuCoin was also charged with operating an unlicensed MTB and a substantive violation of the BSA.

97. The DOJ and DHS alleged, among other things, that KuCoin deliberately chose not to help identify and drive out crime and corrupt financing schemes, failed to implement even basic AML policies, and allowed KuCoin to be used as "a haven for illicit money laundering, with KuCoin receiving over $5 billion and sending over $4 billion of suspicious and criminal funds."

98. The March 26, 2024 press release jointly issued by the DOJ and DHS, which announced the unsealing of an Indictment against KuCoin, Gan, and Tang (the "DOJ Indictment"), stated in pertinent part as follows:

> **KuCoin and Two of Its Founders, Chun Gan and Ke Tang, Flouted U.S. Anti-Money Laundering Laws to Grow KuCoin Into One of World's Largest Cryptocurrency Exchanges**
>
> Damian Williams, the United States Attorney for the Southern District of New York, and Darren McCormack, the Acting Special Agent in Charge of the New York Field Office of Homeland Security Investigations ("HSI"), announced today the ***unsealing of an Indictment*** against global cryptocurrency exchange KuCoin and two of its founders, CHUN GAN, a/k/a "Michael," and KE TANG, a/k/a "Eric," ***for conspiring to operate an unlicensed money transmitting business and conspiring to violate the Bank Secrecy Act by willfully failing to maintain an adequate anti-money laundering ("AML") program designed to prevent KuCoin from being used for money laundering and terrorist financing, failing to maintain reasonable procedures for verifying the identity of customers, and failing to file any suspicious activity reports. KuCoin was also charged with operating an unlicensed money transmitting business and a substantive violation of the Bank Secrecy Act***. GAN and TANG remain at large.
>
> ***U.S. Attorney Damian Williams said***: "As today's Indictment alleges, ***KuCoin and its founders deliberately sought to conceal the fact that substantial numbers of U.S. users were trading on KuCoin's platform***. Indeed, KuCoin allegedly took advantage of its sizeable U.S. customer base to become one of the world's largest cryptocurrency derivatives and spot exchanges, with billions of dollars of daily trades and trillions of dollars of annual trade volume. But financial institutions like KuCoin that take advantage of the unique opportunities available in the United States must also comply with U.S. law to help identify and drive out crime and corrupt financing schemes. KuCoin allegedly deliberately chose not to do

> so. As alleged, ***in failing to implement even basic anti-money laundering policies, the defendants allowed KuCoin to operate in the shadows of the financial markets and be used as a haven for illicit money laundering, with KuCoin receiving over $5 billion and sending over $4 billion of suspicious and criminal funds***. Crypto exchanges like KuCoin cannot have it both ways. ***Today's Indictment should send a clear message to other crypto exchanges: if you plan to serve U.S. customers, you must follow U.S. law, plain and simple***."
>
> ***HSI Acting Special Agent in Charge Darren McCormack said***: "Today, ***we exposed one of the largest global cryptocurrency exchanges for what our investigation has found it to truly be: an alleged multibillion-dollar criminal conspiracy***. KuCoin grew to service over 30 million customers, despite its alleged failure to follow laws necessary to ensuring the security and stability of our world's digital banking infrastructure. ***The defendants' alleged pattern of skirting these vitally important laws has finally come to an end***. I commend HSI New York's El Dorado Task Force and our law enforcement partners for their commitment to the mission."
>
> * * *
>
> Mr. Williams praised the outstanding investigative work of HSI New York's El Dorado Task Force. Mr. Williams further thanked the Commodity Futures Trading Commission, which today filed a parallel civil action against KuCoin.
>
> ***This matter is being handled by the Office's Illicit Finance & Money Laundering Unit***. Assistant U.S. Attorneys Emily Deininger and David R. Felton are in charge of the prosecution.

99. The DOJ Indictment alleged the following, among other things, against KuCoin and the Individual Defendants:

(a) KuCoin, Gan, and Tang sought to serve, and have in fact served, numerous customers located in the United States and in the Southern District of New York.

(b) As a result, KuCoin has, from inception, been an MTB required to register with FinCEN and, since July 2019, has been an FCM required to register with the CFTC.

(c) As an MTB and an FCM merchant, KuCoin is required to comply with the applicable BSA provisions requiring maintenance of an adequate AML program, including customer identity verification, or KYC processes.

(d) Gan, Tang, and KuCoin were aware of their U.S. AML obligations but willfully chose to flout those requirements. KuCoin failed, for example, to implement an adequate KYC program.

(e) Until at least July 2023, KuCoin did not require customers to provide any identifying information. It was only in July 2023, after KuCoin was notified of a federal criminal investigation into its activities, that KuCoin belatedly adopted a KYC program for new customers. However, this KYC process applied to new customers only and did not apply to KuCoin's millions of existing customers, including the substantial number of customers based in the United States.

(f) KuCoin never filed any required suspicious activity reports, never registered with the CFTC as an FCM, and, through at least the end of 2023, never registered with FinCEN as an MTB.

(g) Gan, Tang, and KuCoin affirmatively attempted to conceal the existence of KuCoin's U.S. customers to make it appear as if KuCoin was exempt from U.S. AML and KYC requirements. Despite the fact that KuCoin gathered and tracked location information for its customers, KuCoin actively prevented its U.S. customers from identifying themselves as such when opening KuCoin accounts.

(h) In a number of social media posts, KuCoin actively marketed itself to U.S. customers as an exchange where they could trade without having to undergo KYC. For example, KuCoin stated in an April 2022 message on Twitter that "KYC is not supported to USA users, however, it is not mandatory on KuCoin to do KYC. Usual transactions can be done using an unverified account . . . ."

(i) As a result of KuCoin's willful failures to maintain the required AML and KYC programs, KuCoin has been used as a vehicle to launder large sums of criminal proceeds,

including proceeds from darknet markets and malware, ransomware, and fraud schemes. Since its founding in 2017, KuCoin has received over $5 billion, and sent over $4 billion, of suspicious and criminal proceeds. Many KuCoin customers used its trading platform specifically because of the anonymity of the services it provided. In other words, KuCoin's no-KYC policy was integral to its growth and success.

The CFTC Action Against KuCoin

100. On March 26, 2024, the CFTC issued a press release and announced it had filed a civil enforcement action in the U.S. District Court for the Southern District of New York charging Mek Global, PhoenixFin, Flashdot, and Peken Global with multiple violations of the CEA and CFTC regulations. The CFTC press release stated in pertinent part as follows:

> The complaint charges KuCoin illegally dealt in off-exchange commodity futures transactions and leveraged, margined, or financed retail commodity transactions; solicited and accepted orders for commodity futures, swaps, and leveraged, margined, or financed retail commodity transactions without registering with the CFTC as a futures commission merchant (FCM); failed to diligently supervise its FCM activities; operated a facility for the trading or processing of swaps without registering with the CFTC as a swap execution facility (SEF) or designated contract market (DCM); and failed to implement an effective customer identification program (CIP).
>
> In its continuing litigation against KuCoin, the CFTC seeks disgorgement, civil monetary penalties, permanent trading and registration bans, and a permanent injunction against further violations of the CEA and CFTC regulations, as charged.
>
> "For too long, some offshore crypto exchanges have followed a now-familiar playbook by offering derivative products and ***falsely claiming people in the United States cannot use their platforms, when in reality, anyone in the U.S. with commonly used technology can trade without providing basic customer identifying information***," said Director of Enforcement Ian McGinley.
>
> "As made clear by the CFTC's action today and its previous enforcement actions, the CFTC's playbook should also now be familiar – the CFTC will charge such entities with failing to register with the CFTC and ***failing to comply with the agency's rules that protect U.S. customers and prevent and detect terrorist financing and money laundering***," McGinley continued.

Case Background

According to the complaint, KuCoin offered and executed commodity derivatives and leveraged, margined, or financed commodity transactions to and for people in the U.S. ***from approximately July 2019 to approximately June 2023, and failed to implement required know-your-customer (KYC) compliance procedures. The complaint further alleges that although KuCoin claimed to have implemented KYC procedures, those procedures were a sham and did not prevent U.S. customers from trading commodity interests and derivatives on the platform***.

The complaint also alleges people who identified themselves as being U.S. customers were permitted to trade commodity futures, swaps, and leveraged, margined, or financed commodity transactions on the exchange, in violation of the CEA and CFTC regulations. ***KuCoin failed to impose any IP address restrictions during the relevant period to prevent U.S. customers from trading commodity interests or account for commonly used technology such as virtual private networks (VPNs) that could potentially circumvent IP address restrictions***.

Related Criminal Action

In a separate criminal matter, the U.S. Attorney's Office for the Southern District of New York filed an indictment against PhoenixFin PTE Ltd., Flashdot Limited, and Peken Global Limited charging them with violating the Bank Secrecy Act, operating an unlicensed money transmitter business, and conspiracy to violate the Bank Secrecy Act and operate as an unlicensed money transmitter business.

101. The complaint filed by the CFTC (the "CFTC Complaint") alleges, among other things, that: (i) KuCoin failed to restrict U.S. customers' access to KuCoin's exchange from at least July 2019 and continuing to at least June 2023; (ii) KuCoin's KYC verification was a sham; (iii) KuCoin publicly encouraged U.S. persons to avoid its KYC process; (iv) KuCoin engaged in marketing activities targeting U.S. persons; and (v) KuCoin sought U.S.-based investors and employees.

102. Furthermore, the CFTC Complaint alleges, among other things, that from at least July 2019 and continuing to at least June 2023, KuCoin violated core provisions of the CEA and CFTC regulations, including:

(a) offering, entering into, confirming the execution of, or otherwise dealing in, off-exchange commodity futures transactions or transactions described in §2(c)(2)(D) of the CEA, in

violation of §4(a) of the CEA, 7 U.S.C. §6(a), or, alternatively, §4(b) of the CEA, 7 U.S.C. §6(b), and Regulation 48.3, 17 C.F.R. §48.3;

(b) soliciting and accepting orders for commodity futures, swaps, and retail commodity transactions or acting as a counterparty in any agreement, contract, or transaction described in §2(c)(2)(D)(i) of the CEA; and, in connection with these activities, accepting money, securities, or property (or extending credit in lieu thereof) to margin, guarantee, or secure resulting trades on KuCoin, without registering as an FCM, in violation of §4d of the CEA, 7 U.S.C. §6d;

(c) operating a facility for the trading or processing of swaps without being registered as a swap execution facility or designated contract market, in violation of §5h(a)(1) of the CEA, 7 U.S.C. §7b-3(a)(1), and Regulation 37.3(a)(1), 17 C.F.R. §37.3(a)(1);

(d) failing to diligently supervise KuCoin's activities relating to the conduct that subjects KuCoin to CFTC registration requirements, in violation of Regulation 166.3, 17 C.F.R. §166.3; and

(e) failing to implement an effective customer identification program and to otherwise comply with applicable provisions of the BSA, in violation of Regulation 42.2, 17 C.F.R. §42.2.

103. The CFTC Complaint alleges that Regulation 42.2, 17 C.F.R. §42.2, requires, among other things, that every FCM shall comply with the applicable provisions of the BSA and the regulations promulgated by the U.S. Department of the Treasury under the BSA at 31 C.F.R. chapter X, and with the requirements of 31 U.S.C. §5318(l) and the implementing regulation jointly promulgated by the CFTC and the U.S. Department of the Treasury at 31 C.F.R. §1026.220, which require that a customer identification program be adopted as part of the firm's BSA compliance program.

KuCoin Paid $22 Million to Settle the NYAG's Claims

104. On December 12, 2023, the NYAG issued a press release announcing that NYAG Letitia James "secured ***more than $22 million from KuCoin***" for failing to register as a securities and commodities broker-dealer and for falsely representing itself as a crypto exchange. The December 12, 2023 stipulation and consent order in connection with the settlement, entered into by Mek Global and PhoenixFin and the State of New York (the "NYAG Consent Order"), resolved Attorney General James' March 9, 2023 lawsuit against KuCoin and required KuCoin to refund to over 150,000 New York investors more than $16.7 million and pay more than $5.3 million to New York State. KuCoin was also banned from trading securities and commodities in New York and from making its platform available to New Yorkers. The press release also stated in pertinent part as follows:

> "Unregistered offshore crypto platforms pose a risk to investors, consumers, and the broader economy," said Attorney General James. "Crypto companies should understand that they must play by the same rules as other financial institutions, and my office will hold them accountable when they don't. This settlement will ensure every New Yorker who put their money into KuCoin can get it back and that KuCoin won't be able to put other New York investors at risk. I will continue to take action against any company that brazenly disregards the law and jeopardizes New Yorkers' savings and investments."
>
> KuCoin is a Seychelles-based cryptocurrency trading platform that allows investors to buy and sell cryptocurrency through its website and mobile app. An investigator from the Office of the Attorney General (OAG) was able to create an account with KuCoin using a computer with a New York-based IP address to buy and sell cryptocurrencies, including popular tokens like ETH, LUNA, and UST. However, New York law requires securities and commodities brokers providing services in New York to register with the state, which KuCoin failed to do. By trading cryptocurrencies that are commodities and securities with its New York users, KuCoin violated state law. This included its own "KuCoin Earn" investment product, in which KuCoin pooled investors' cryptocurrencies to generate income for its investors.
>
> In addition, KuCoin claimed to be an exchange, but was not registered with the Securities and Exchange Commission as a national securities exchange or appropriately designated by the Commodity Futures Trading Commission as is required under New York Law.

105. KuCoin admitted to the following facts, among others, in the NYAG Consent Order:

(a) KuCoin admits that it operates a cryptocurrency trading platform on which users, including users in New York State, can purchase and sell cryptocurrencies that are securities or commodities as defined under the laws of New York State and that KuCoin is not registered in New York State as a securities or commodities broker-dealer;

(b) KuCoin admits that it represented itself as an "exchange" and was not registered as an exchange pursuant to the laws of New York State; and

(c) while subject to market fluctuation, KuCoin attests that as of November 29, 2023, New York customers held assets with an approximate notional value of $16,766,642 worth of fiat and/or cryptocurrencies at KuCoin.

106. Defendants ignored the laws of foreign jurisdictions in which KuCoin operated as well. According to the NYAG verified petition, at least three foreign jurisdictions have taken adverse regulatory action against KuCoin, including the following:

(a) in February 2021, the Financial Services Authority of the Republic of Seychelles identified Mek Global as operating a cryptocurrency trading platform under the name KuCoin and through the KuCoin website without proper licensure and, as a result, removed the company from the Seychelles corporate registry;

(b) in June 2022, the Ontario Securities Commission ("OSC") obtained a multimillion-dollar judgment in a proceeding against Mek Global and PhoenixFin finding that KuCoin operated in Ontario without properly registering, in the action *In re MEK Global Limited and PhoenixFin Pte. Ltd.*, 2022 ONCMT 15 (June 21, 2022); and

(c) in December 2022, the Central Bank of the Netherlands issued a warning to investors regarding Mek Global doing business as KuCoin. The warning concerned KuCoin offering

services without registration, including exchanging virtual currencies and illegally offering custodian wallets.

Background on Cryptocurrency Laundering

107. A cryptocurrency wallet is an application that functions as a wallet for cryptocurrency. It is referred to as a wallet because it is used similarly to a physical wallet in which cash and credit cards are placed. Instead of holding physical items, it stores the passkeys a cryptocurrency holder uses to sign for their cryptocurrency transactions and provides the interface that lets the user access their crypto on the blockchain, and interact with protocols, such as decentralized exchanges ("DEX") and bridges, which enable users to send crypto across different blockchains. When someone sends their cryptocurrency to another wallet on the blockchain or engages with a protocol, such as a DEX or bridge, a permanent record is created on the ledger for the blockchain so all transactions on the blockchain are trackable.

108. Blockchain transactions are inherently immutable and transparent. They are recorded on digital ledgers distributed across a decentralized network of nodes. These transactions, encompassing details such as sender and recipient addresses, transaction amounts, and timestamps, are permanently recorded, ensuring the integrity and security of the data. If a bad actor removes someone's crypto without their permission from their wallet or a protocol and then transfers the crypto to the bad actor's own wallet or tries to withdraw the funds as fiat currency to a bank account, the bad actor could potentially be caught by experts who employ tools and services to trace the movement of stolen digital assets, facilitating potential recovery. Therefore, unlike cash or other types of fungible property, cryptocurrency can be tracked (within limits) after it is removed from the owner's wallet or protocol.

109. After cryptocurrency is stolen, with the assistance of forensic experts, victims are regularly able to locate the precise location of their assets through the public ledger on the

blockchain. Therefore, even though their cryptocurrency may have been stolen, victims often have a strong ability to track and potentially recover their stolen assets as long as the information is trackable on the blockchain.

110. A February 1, 2023 article published on defendant Chainalysis' website, titled "2022 Biggest Year Ever For Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers," discussed the tracking benefits of the blockchain, stating, in pertinent part, as follows:

> When every transaction is recorded in a public ledger, it means that law enforcement always has a trail to follow, even years after the fact, which is invaluable as investigative techniques improve over time. Their growing capabilities, combined with the efforts of agencies like OFAC to cut off hackers' preferred money laundering services from the rest of the crypto ecosystem, means that these hacks will get harder and less fruitful with each passing year.

111. As such, laundering cryptocurrency, *i.e.*, the removal of the ability for the stolen cryptocurrency to be tracked on the ledger, is essential for a criminal to benefit from the theft without detection and eliminates a victim's ability to recover their stolen cryptocurrency.

112. The 2022 Crypto Crime Report by defendant Chainalysis highlights the importance of crypto-laundering as part of the overall theft:

> Cybercriminals dealing in cryptocurrency share one common goal: Move their ill-gotten funds to a service where they can be kept safe from the authorities and eventually converted to cash. ***That's why money laundering underpins all other forms of cryptocurrency-based crime. If there's no way to access the funds, there's no incentive to commit crimes involving cryptocurrency in the first place***.

113. The KuCoin Crypto-Wash Enterprise provided an effective way for bad actors to steal and launder crypto. Once someone steals crypto stored in a wallet or protocol, they would deposit the stolen cryptocurrency into their KuCoin wallet. Next, they would engage in transactions within the exchange, trading the stolen cryptocurrency for other cryptocurrencies or tokens offered on the platform. Once the funds were sufficiently converted, the thief would withdraw them from the

exchange, potentially through multiple accounts or wallets, to further complicate tracing efforts. By leveraging the anonymity and liquidity provided by the KuCoin Crypto-Wash Enterprise, individuals laundered cryptocurrency and evaded detection.

114. Before the laundering, victims had a considerable likelihood of recovering their stolen cryptocurrency assets with the cooperation of the authorities. The laundering of the stolen cryptocurrency, however, eliminated their ability to track and potentially recover their assets. In other words, those victims lost any chance to track and recover their stolen assets.

115. The KuCoin Defendants' purposeful refusal to implement AML and KYC policies and protocols at KuCoin affirmatively enabled bad actors to launder crypto at KuCoin. Had the KuCoin Defendants complied with the law and ensured KuCoin had necessary AML and KYC policies, bad actors would not have been drawn to KuCoin to launder crypto or, if the bad actors had, they would have been prevented from laundering stolen crypto through KuCoin, or KuCoin and the authorities would have been able to identify the bad actors and/or track the stolen assets that were withdrawn from KuCoin. At a minimum, Plaintiffs and members of the Class would not have lost the ability to trace and potentially recover their stolen assets.

116. A key reason for this is because a substantial portion of crypto laundered by bad actors were transferred to KuCoin from crypto wallets ***previously identified as wallets associated with illicit crypto activities***. In fact, a January 18, 2024 *Reuters* article titled "Illicit crypto addresses received at least $24.2 billion in 2023 – report" stated: "At least $24.2 billion worth of crypto was sent to illicit crypto wallet addresses in 2023, including addresses identified as sanctioned or linked to terrorist financing and scams, crypto research firm Chainalysis said . . . ."

KuCoin Marketed Its Exchange to U.S. Customers

117. The KuCoin Defendants engaged in substantial marketing and solicitation efforts to acquire users based in the United States, and KuCoin's tremendous growth rate and revenues were due in large part to its U.S.-based users.

118. KuCoin had an affiliate program that rewarded customers with trading fee commissions for referring other customers. According to the CFTC Complaint, many of the 16,000 participants in KuCoin's affiliate program were based in the United States, including users on U.S.-based social media platforms such as X (formerly known, and hereinafter referred to, as "Twitter") and YouTube. Similar to the affiliate program, in July 2020, KuCoin launched the KuCoin Futures Global Influencer Program, which offered key social media influencers referral commissions of up to 40% of the trading fees generated by new customers. KuCoin provided participants in the affiliate program and Futures Global Influencer Program with hyperlinks that could be added to their websites or social media content, which enabled KuCoin to track the referrals and run the program.

119. According to the CFTC Complaint, since at least August 2021, KuCoin worked with a Toronto, Canada-based marketing firm to execute an "influencer campaign" to target "English" markets, including the United States. The influencer campaigns included YouTube videos that KuCoin promoted on its website as "Top YouTubers," which included U.S.-based YouTubers who admitted to trading on KuCoin and encouraged others to do the same. On or about June 21, 2022, the Ontario Capital Markets Tribunal issued a Reasons and Decisions in an action brought by the OSC against KuCoin in which the OSC obtained a multimillion-dollar judgment against KuCoin because it operated in Ontario without properly registering, in the action titled *In re MEK Global Limited and PhoenixFin Pte. Ltd.*, 2022 ONCMT 15 (June 21, 2022).

120. KuCoin had millions of U.S.-based customers, including many customers in New York. Throughout much of the Class Period, KuCoin had more customers based in the United States

than any other nation in the world. According to the DOJ Indictment, in or about May 2018, KuCoin sent an email to a potential investor, which represented that approximately 17% of KuCoin's customers were located in the United States, more than double the number of customers from any other country in the world. Defendants Gan and Tang were copied on that email and were therefore aware that the email represented that KuCoin had more customers in the United States than in any other country. According to the DOJ Indictment, a third-party analysis of digital traffic showed that approximately 19% of visits to KuCoin's website, www.KuCoin.com, were from individuals in the United States.

121. KuCoin actively marketed its exchange to obtain customers based in the United States. KuCoin employees regularly attended cryptocurrency conferences in the United States, including in New York. In June 2022, KuCoin's CEO and other high-level KuCoin executives attended the Consensus 2022 conference held in Austin, Texas, which KuCoin sponsored, according to the CFTC Complaint. According to the DOJ Indictment and the CFTC Complaint, KuCoin hosted an information booth at the Consensus 2022 conference.

122. In or about June 2022, KuCoin was a sponsor of NFT.NYC 2022, a conference in Manhattan regarding non-fungible tokens ("NFTs"). Between July 26 and 28, 2022, KuCoin, through its KuCoin Pool product, was a sponsor of Mining Disrupt 2022 in Miami, Florida, a cryptocurrency mining event. In September 2022, KuCoin sponsored an after-party event related to the Mainnet 2022 crypto-industry summit at High Bar New York, located in New York City.

123. Between KuCoin's launch in 2017 and until at least the date of the DOJ Indictment, which was unsealed on or about March 26, 2024, each of the KuCoin Defendants have actively sought to serve, and have served, thousands of customers located in the United States, and until

December 2023, actively sought to serve and have served customers located in the Southern District of New York, according to the DOJ Indictment.

KuCoin Sought U.S.-Based Investors and Employees

124. In 2022, KuCoin raised over $150 million in investments through a Series B round of funding, bringing total investments to $170 million when combined with a Series A funding round of approximately $20 million in 2018. Four of KuCoin's seven investors have offices or headquarters in the United States. During its Series A funding, KuCoin openly touted its U.S. customer base, telling investors that 20% to 50% of its customers were from the United States, according to the CFTC Complaint.

125. According to the CFTC Complaint, over 100 KuCoin employees resided in the United States during the Class Period, representing more than 10% of KuCoin's employees in 2022 and the largest concentration of KuCoin's workforce.

126. According to the CFTC Complaint, KuCoin employees, including the "Head of Futures," numerous project managers, officers, directors, and coordinators listed a U.S. residence.

The KuCoin Defendants Knew KuCoin Had a Substantial Number of U.S.-Based Customers but Failed to Require KYC Information or Implement AML Procedures

127. Defendants knew that a substantial number of KuCoin's customers were based in the United States and that KuCoin did not prohibit customers in the United States from opening and using KuCoin accounts.

128. The KuCoin Defendants collected the location information from KuCoin's customers, including IP address information from the devices used by customers to access KuCoin. According to the DOJ Indictment, the "IP address information collected by KuCoin demonstrated that KuCoin customers were accessing KuCoin using U.S.-based IP addresses."

129. In fact, during the plea and sentencing hearing in connection with the DOJ Indictment, defendant Peken Global admitted that "[s]ince its launch, KuCoin has served approximately 1.5 million registered users located in the United States."

130. KuCoin maintained login history for its customers, which included location information under the heading "Login Region." According to the DOJ Indictment, "an email sent from KuCoin to a U.S. customer on or about November 14, 2022 notified the customer that he had logged in from 'United States Bridgehampton [New York]'" and that KuCoin "included customer IP address information, including U.S.-based IP addresses, in emails sent to KuCoin customers for verification purposes in connection with customer withdrawals."

131. Furthermore, each of the Individual Defendants received automated emails from KuCoin while they were in the United States, which reflected that each of the Individual Defendants were logging into KuCoin from the United States, including Tang's receipt of an email on or about January 2021 reflecting he had logged in from Los Angeles, California; and on or about January 2019, Gan's receipt of an email confirming he had logged in from San Mateo, California. Therefore, KuCoin and the Individual Defendants knowingly failed to restrict access to KuCoin by users located in the United States.

132. Defendants understood that KuCoin was subject to U.S. AML and KYC requirements. For example, according to the DOJ Indictment, KuCoin's CEO publicly acknowledged in a post on Reddit.com in or about October 2021 that KuCoin "keep[s] a close eye on the regulation changes in every market we operate." Also, according to the DOJ Indictment, in or about May 2018, defendant Gan confirmed his knowledge of FinCEN registration requirements when he responded, "[w]e haven't [sic] a FinCEN registration yet" in response to a request by a

representative from a financial services company for Gan to provide KuCoin's "FinCEN registration as a money transmitter given your company serves US citizens."

133. Even though the KuCoin Defendants each knew that KuCoin served a substantial number of customers based in the United States, the KuCoin Defendants failed to register KuCoin with the CFTC as an FCM and failed to register KuCoin with FinCEN as an MTB.

134. Additionally, the KuCoin Defendants willfully failed to implement AML or KYC policies and procedures and permitted U.S.-based KuCoin users to open accounts and use KuCoin's exchange without providing sufficient identifying information or documents to allow KuCoin to form a reasonable belief that it knew the true identity of its customers.

135. Prior to on or about July 15, 2023, KuCoin customers could register to trade on KuCoin anonymously, by providing only an email address and without providing any identifying information or documentation.

136. In fact, KuCoin employees regularly and frequently stated on public social media websites that KYC was not mandatory on KuCoin, including in response to posts from customers who had identified themselves as being in the United States.

137. The DOJ Indictment identified the following KuCoin Moderator post:

138. KuCoin actively prevented its customers based in the United States from identifying themselves as U.S. customers when establishing KuCoin accounts. The KuCoin Defendants sought to conceal the existence of KuCoin's U.S.-based customers to make it appear as if KuCoin was exempt from U.S. AML and KYC laws and regulations.

139. For example, KuCoin offered customers an optional identification verification process that, once completed, granted customers access to additional features, such as larger daily withdrawals. According to the DOJ Indictment, despite knowing that many users were in the United States, KuCoin did not include the United States as a possible country for selection by customers in the optional verification process, which prevented U.S. customers from being able to identify themselves as such.

140. KuCoin publicly encouraged U.S. customers to use its service and avoid its purported KYC process to maximize users and revenues.

141. According to the CFTC Complaint, KuCoin's customer support repeatedly told customers who attempted to complete KYC verification from the United States that they could continue to trade on KuCoin as an unverified customer, such that they did not need to submit any KYC information. In other words, even though KuCoin issued public statements indicating that the KuCoin platform was not approved for U.S.-based users, such statements were made with a wink and a nod, along with instructions for how U.S.-based users could still use the KuCoin platform. According to the CFTC Complaint, although KuCoin paid lip service to the notion that it "must adhere to relative regulation and laws to stop providing service for those customers whose KYC show that they are the citizens" of prohibited countries, KuCoin did not terminate unverified accounts with known U.S.-based trading activity or prohibit those accounts from trading commodity derivatives.

142. Furthermore, a large number of U.S. customers publicly identified themselves on social media as KuCoin customers and interacted with KuCoin customer support representatives relating to KYC verification. According to the CFTC Complaint, customer support at KuCoin instructed potential users that trading from the United States was permissible and that they could access the platform simply by declining to complete the KYC verification process.

143. KuCoin representatives responded to questions from U.S. users in the subreddit forum "r/KuCoin" on Reddit.com and confirmed that the platform was available to U.S. customers without any KYC. According to the CFTC Complaint, a KuCoin moderator on the subreddit stated: "KYC is not supported [in the U.S.] but you can still all [sic] features of KuCoin with unverified account."

144. According to the DOJ Indictment, in or about April 2022, a prospective customer posted on Twitter that he was "in the United States" and that his attempt to use KuCoin's optional verification process had failed. In response, a KuCoin representative wrote that while "users from the USA is not supported for KYC service," "[r]est assured that you are not obliged to do KYC on KuCoin."

145. The CFTC Complaint identified other posts by KuCoin in the subreddit, including the following:

> Out of respect to the company's operational requirements, we are only providing service for countries listed in the KYC countries list (US is not included), in order to comply with all applicable laws and regulations. If a user's country is not included in the list, unfortunately, we are temporarily unable to verify the user's KYC. Rest assured that on KuCoin, KYC it is not mandatory, you can still do transactions even if you are not verified yet.
>
> * * *
>
> [R]est assured that US residents can use KuCoin even KYC [sic] is not supported. Please be noted [sic] that KYC is not mandatory here in KuCoin. However, you'll have some limitations for being [an] "unverified" account.

146. KuCoin communicated with U.S.-based users through Twitter during the Class Period and advised them to avoid providing KYC information.

147. In or about February 2022, according to the DOJ Indictment, a user on Reddit.com asked: "Will Kucoin ever follow U.S. KYC/AML requirements?" In response, a KuCoin representative stated that "we are only providing service for countries listed in the KYC countries list (US is not included), in order to comply with all applicable laws and regulations," but further explained that "you may still perform all functions on our exchange as normal" except that "[t]here will be individual account's daily withdrawal limitation of 5 BTC [Bitcoin]" and potential limitations on other activities.

148. The CFTC Complaint identified numerous communications between KuCoin and U.S. users, including the following:

(a) in response to a complaint in April 2022 about difficulties signing up from the United States, the KuCoin moderator stated: "KYC is not supported to [sic] USA users, however, it is not mandatory on KuCoin to do KYC. Usual transactions can be done using an unverified account";

(b) in April 2022, a Twitter user stated that he was "in the United States" and asked KuCoin to tell him "why [his] KuCoin account is saying Verification Failed after [he] used it several times two weeks ago." KuCoin responded: "Users from the USA is [sic] not supported for KYC service. Rest assured that you are not obliged to do KYC on KuCoin";

(c) KuCoin told U.S. customers that "[n]ormal transfers and trade behaviors will not be limited" for unverified accounts;

(d) a customer claiming to be based in San Antonio wrote on Twitter: "@kucoincom A few hours ago I was trading futures on your mobile app when the system logged me out"; and

(e) a customer claiming to be based in California wrote on Twitter: "@kucoincom isolated margin just literally made money disappear."

149. The numerous communications between KuCoin and users based in the United States through Reddit and Twitter show that KuCoin was fully aware its platform was being actively used by customers in the United States.

150. According to the CFTC Complaint, a YouTube video linked on the KuCoin website and sponsored by KuCoin listed the top seven reasons to use the KuCoin platform. The number one reason to use the platform according to the YouTube user was that KYC verification was optional. The YouTube user also stated that U.S. customers were not eligible for KuCoin's KYC verification process but that U.S. customers could use the platform nevertheless.

151. Even though a portion of KuCoin's users may have been legitimate, Defendants' conduct turned KuCoin into a magnet and hub for bad actors to use KuCoin to launder stolen cryptocurrency; and this portion of KuCoin's business served as the KuCoin Crypto-Wash Enterprise. Defendants and co-conspirators knew that KuCoin's failure to comply with KYC and AML procedures enabled bad actors, including criminals, crypto-thieves, and users located in sanctioned jurisdictions to use the KuCoin Crypto-Wash Enterprise to launder their digital assets so the assets would not be trackable by the authorities.

152. According to the DOJ Indictment: "KuCoin lied to at least one investor regarding the geographic location of its customers, falsely representing that it had no U.S. customers, when in truth

and in fact, KuCoin and its executives, including Gan and Tang, knew that KuCoin's customer base included a substantial portion of customers based in the United States."

153. Eventually, on or about July 15, 2023, KuCoin belatedly and purportedly adopted a KYC program requiring verification of identities. According to the DOJ Indictment, KuCoin only adopted this KYC program after a KuCoin investor and a financial services company notified KuCoin of a federal criminal investigation into its activities.

154. According to a KuCoin press release on June 28, 2023, "[s]tarting from July 15, 2023, all newly registered users must complete KYC to access KuCoin's comprehensive suite of products and services." Additionally, KuCoin announced: "For users who registered before July 15, 2023, failure to complete the KYC process will restrict their access to certain features. Specifically, these users can only utilize services such as Spot trading sell orders, Futures trading deleveraging, Margin trading deleveraging, KuCoin Earn redemption, and ETF redemption."

155. Even though KuCoin purported to implement a KYC program during 2023, a substantial number of U.S.-based users continued using KuCoin's platform without providing KYC information – thus demonstrating KuCoin's KYC program was inadequate and not compliant with the BSA.

156. Indeed, as KuCoin admitted on or about December 8, 2023 in the NYAG Consent Order, as of November 29, 2023, KuCoin held approximately $16,766,642 in assets for New York customers. These New York customers were identified based on a New York address, phone number, or IP address or GPS location in KuCoin's records. Therefore, even though KuCoin purported to "block" U.S. customers from using its website, U.S.-based users continued accessing its platform.

The KuCoin Defendants' Failure to Implement KYC and AML Procedures Enabled Bad Actors to Launder Crypto at the KuCoin Crypto-Wash Enterprise

157. Each of the KuCoin Defendants' willful failures to implement KYC and AML policies and procedures caused KuCoin to be used by bad actors as a vehicle for laundering cryptocurrency. Because the KuCoin Defendants failed to implement an adequate KYC or AML program, KuCoin could not and did not monitor its customer transactions for money laundering, terrorist financing, and sanctions violations. Throughout the Class Period, bad actors repeatedly used KuCoin to launder cryptocurrency.

158. The DOJ Indictment listed several examples of the laundering of cryptocurrency at KuCoin as a direct result of the KuCoin Defendants' failure to implement BSA-compliant AML and KYC programs, including the following:

(a) since its founding, KuCoin received more than $5.39 billion and transmitted more than $4.09 billion of suspicious and criminal proceeds;

(b) from at least in or about 2020 through at least in or about 2022, KuCoin was used to launder the proceeds of a wire fraud and bank fraud scheme that operated for over two years and in which millions of dollars were stolen from U.S. banks and other cryptocurrency exchanges; and

(c) between in or about August 8, 2022 and in or about November 2023, almost 197 KuCoin deposit addresses directly or indirectly received a total of more than $3.2 million worth of cryptocurrency from Tornado Cash, a virtual currency mixer that was designated by the Office of Foreign Assets Control as a Specially Designated National ("SDN") on August 8, 2022 because it was used to launder the proceeds of cybercrimes. This SDN designation prohibited U.S. persons or persons within the United States from transacting with Tornado Cash.

159. According to the DOJ Indictment, since its launch, KuCoin has failed to file any reports of suspicious transactions to the U.S. Department of the Treasury as required by 31 U.S.C. §5318(g) and 31 C.F.R. §§1026.320 and 1022.320.

Plaintiffs and the Class Suffered Financial Harm from the KuCoin Crypto-Wash Enterprise

160. As a result of Defendants' conduct and KuCoin's systemic failures to require KYC and implement AML procedures, Plaintiffs and the Class members have been damaged.

161. For example, between May 21, 2021 and May 22, 2021, ten different cryptocurrencies, which were housed on U.S. servers, were stolen from plaintiff Reca while she resided in the U.S.:

Coin	Theft Date (UTC)	Theft TX Hash	Receiving Address	Volume	USD Value on Date of Theft [approx.]
BTC	05/21/2021 12:52	7d531bb536a835a0a622c821dd2ccf214cde9e6f5448c9c56ce90f35cf8fcf02	12qjL74E87H6wNPH2RXXkrpcrL9Jidomx	2.92939337	$120,329.23
ETH	05/21/2021 12:51	0x861c323f30759dc704d2bda6d883a543c6d03e4a38143758740cee12159a4a7c	0x7641B0ab4bb72A380B1bFf6eebCfa9bE2A453D4B	178	$495,803.06
USDT	05/21/2021 12:53	0xf092233c5270a4383c2ca5785d8e61d82b9b278182b074a1329b49ab81fba134	0x7641B0ab4bb72A380B1bFf6eebCfa9bE2A453D4B	277,391.7135	$277,391.71
USDT	05/22/2021 17:55	0x2d741e51da12cc64dbb4e39cdb6f4e1c66b28233ddbcd70fb63ca94990de596e	0x7641B0ab4bb72A380B1bFf6eebCfa9bE2A453D4B	99,708.1455	$99,708.15
USDT	05/23/2021 20:21	0xdb7ee9dce723ddcb7d921a0a74a5e690267af251002cb41edc86a355b89b767d	0x7641B0ab4bb72A380B1bFf6eebCfa9bE2A453D4B	382,505.583148	$382,505.58
LTC	05/21/2021 13:26	0e3b37f21b319c689b4382fcf4074c624e3e36c869f07ec8e146e61b69ee7168	LdF6f9c6ZgcTd7VHW3PTKDgk7Yi7Wu8rqM	3.16032571	$644.88
ENJ	05/21/2021 12:53	0x8ceb0dad56724a9c4a589ab59c7f646ee6123c7f8c0147d8a55eff448365ba1c	0x7641B0ab4bb72A380B1bFf6eebCfa9bE2A453D4B	17,006.61701156	$25,322.85

Coin	Theft Date (UTC)	Theft TX Hash	Receiving Address	Volume	USD Value on Date of Theft [approx.]
UNI	05/21/2021 12:54	0xefaae3f3a3bc7548942c5a490d9c1fa89034ca7deefa60172eddacbdb3b3be77	0x7641B0ab4bb72A380B1bFf6eebCfa9bE2A453D4B	383.1837853	$10,119.88
LINK	05/21/2021 12:54	0x4a32cfe34a1245a64eec7dd3ee92d1089856bd87787f41ac3ab170fe14f8d727	0x7641B0ab4bb72A380B1bFf6eebCfa9bE2A453D4B	325.87763304	$10,010.96
DOGE	05/21/2021 12:52	aed514c115da1c865fad1d649a0127fcc67820ee981c02bb2fb0bb5fe6f6f74a	D5avjC2jRa3RpX4MHfBdQuGATLP6jgE3mb	26387.339997	$10,536.46
MATIC	05/21/2021 13:11	0x5b8134aceee670c4c8a12a4970b9d3896e2a390b4c861df6d5989fd5e6dd20d8	0x7641B0ab4bb72A380B1bFf6eebCfa9bE2A453D4B	2271.088759	$4,153.82
AAVE	05/21/2021 13:11	0xab713b9397851dd5e752ccafb99a57be3530120f88d6670ba5d95902b303c210	0x7641B0ab4bb72A380B1bFf6eebCfa9bE2A453D4B	2.26884	$1,061.41
USDC	05/21/2021 13:11	0xdf7bfbfd01369412cf7fb6221706f88c1e55831200c98d1ca34b6162a935a981	0x7641B0ab4bb72A380B1bFf6eebCfa9bE2A453D4B	198.13	$198.13
					TOTAL: $1,437,786.12

162. After tracing several of the above-identified assets and determining that some of them were converted into other cryptocurrency assets, expert cryptographic tracers concluded that between May 2021 and July 2021 many of plaintiff Reca's stolen assets were transferred in a series of transactions to a collection of deposit addresses at KuCoin (which Defendants could have traced themselves using the KYT protocol) believed to be owned, controlled, or maintained by the John Doe hacker:

BTC - Stolen from Plaintiff Reca and Deposited at KuCoin				
Transaction Hash	**Transfer Date (UTC)**	**Sending Address**	**Receiving Address at KuCoin**	**Volume**
3baca720e0b5281d20891cd88754849cdec12f4dbdb3c45298501bd6e75cb071	06/06/2021 09:29	12qjL74E87H6wNNPH2RXXkrpcrL9Jidomx	3GiF2FRMptDp9JbbtYjN9oGFLmC1yjDQW8	4.00

ETH - Stolen from Plaintiff Reca and Deposited at KuCoin				
Transaction Hash	**Transfer Date (UTC)**	**Sending Address**	**Receiving Address at KuCoin**	**Volume**
0x8c8e2123a6d8ca29c82ecda5133d9d4dcaf6e68e4ac5ccfbf7b3eb99b61604d0	06/02/2021 22:28	0xF25cF733636dA3F572C0DE99dA10591f55Cc39c9	0x4ad64983349C49dEfE8d7A4686202d24b25D0CE8	0.017232806
0x255754bd8850fea69cadba7d08d9c95a4de93384b38d25570b46ccffead3912e	06/06/2021 10:06	0xF25cF733636dA3F572C0DE99dA10591f55Cc39c9	0x4ad64983349C49dEfE8d7A4686202d24b25D0CE8	149.999538
0x00198f6c1732465e57ae140be827e70025bdb804cd1241fc3c578fa94d21ab45	06/13/2021 04:08	0xF25cF733636dA3F572C0DE99dA10591f55Cc39c9	0x4ad64983349C49dEfE8d7A4686202d24b25D0CE8	49.999643
0x8aa55383d1edbfe82212c7dad1896db083017be9dade08d99336c1b56935d110	07/26/2021 08:30	0xF25cF733636dA3F572C0DE99dA10591f55Cc39c9	0x4ad64983349C49dEfE8d7A4686202d24b25D0CE8	0.018851822

USDT - Stolen from Plaintiff Reca and Deposited at KuCoin				
Transaction Hash	**Transfer Date (UTC)**	**Sending Address**	**Receiving Address at KuCoin**	**Volume**
0x1f71f71c9dc87653b84c969704bc5287c9094e3bea4ec250ede962b3da809c9e	05/22/2021 04:16	0xF25cF733636dA3F572C0DE99dA10591f55Cc39c9	0xa1D8d972560C2f8144AF871Db508F0B0B10a3fBf	175,000
0xf133c91d88370933547049a306a6e7cbaea29ed8d82990fe8ca0b8ef13f326c1	06/23/2021 12:24	0xF25cF733636dA3F572C0DE99dA10591f55Cc39c9	0xe59Cd29be3BE4461d79C0881D238Cbe87D64595A	561,241.156633

ENJ - Stolen from Plaintiff Reca and Deposited at KuCoin				
Transaction Hash	**Transfer Date (UTC)**	**Sending Address**	**Receiving Address at KuCoin**	**Volume**
0x66d0891eb1e5e990a60a0f85182ae0928c6b8d8def0e4458e5d2c05ecfcef3ea	06/13/2021 07:24	0x630321aE72E17e232F53f3DAC5d9cFaA6142a5dE	0xa1D8d972560C2f8144AF871Db508F0B0B10a3fBf	17,000
0x27cac95c6c24bd1362ecb2a600688d984014a313736c5625fd25595df76c379e	06/29/2021 14:56	0xc2c3Ae450662DE36B3992b1490E273F9E57b3Fbd	0xa1D8d972560C2f8144AF871Db508F0B0B10a3fBf	218.558227343
0xc1e193dcc4f6f9cc1f64ece84760d8028ee1b87383f1567cdf1f345aac0988f8	07/10/2021 13:36	0xc2c3Ae450662DE36B3992b1490E273F9E57b3Fbd	0xa1D8d972560C2f8144AF871Db508F0B0B10a3fBf	608.01929112

DOGE - Stolen from Plaintiff Reca and Deposited at KuCoin				
Transaction Hash	**Transfer Date (UTC)**	**Sending Address**	**Receiving Address at KuCoin**	**Volume**
b04b992d20f6219f32226b905	06/13/2021	D5avjC2jRa3RpX4MHf	DFYfPT8hk4WPJQ5FCJ	25,000

03058964272aab65a13bbb359243f6dc1b5af29	05:25	BdQuGATLP6jgE3mb	Eg4c44TA8dnwqPD1	
fcb10ae026c1a3e7e53c5590b0f5793910b03e3ebed43c777d63da21ee8cd9d7	07/04/2021 13:51	DF7tBoxdZPauo7Gt1LUWv6qZi5yiYEZYAW	DNVKqyQH67i8HKccs2SP4oo4of5JundpX4	10,106.778448

163. The crypto taken from plaintiff Supples and transferred to KuCoin during December 2024, as well as the crypto taken from the other members of the Class, followed similar types of paths as those described above.

164. After the cryptocurrency was stolen from Plaintiffs and the other members of the Class, it was traceable on the blockchain so the location of the cryptocurrency could, with the assistance of forensic analysis, be identified and potentially recovered. KuCoin, however, refused to implement adequate KYC and AML policies and procedures, so the bad actors who stole Plaintiffs' and Class members' cryptocurrency were able to launder it through KuCoin. As a result of the laundering of their stolen cryptocurrency through KuCoin, Plaintiffs and the other members of the Class lost the ability to track and potentially recover their stolen cryptocurrency.

165. As a direct and proximate result of KuCoin's policies and failures described herein, Plaintiffs and all Class members suffered financial harm when their digital assets were taken and laundered through KuCoin.

166. As of the date of this filing, Plaintiffs and the members of the Class have not recovered some, if not all, of their stolen cryptocurrency that was transferred to KuCoin.

RICO ALLEGATIONS

167. Defendants engaged in a fraudulent scheme, common course of conduct, and conspiracy to gain market share and generate revenues for KuCoin (and Chainalysis) by enabling bad actors to launder cryptocurrency stolen from the United States through the KuCoin cryptocurrency exchange.

168. To achieve these goals, the KuCoin Defendants set up and managed the KuCoin platform in a manner that willfully violated U.S. laws and regulations requiring adequate KYC or AML policies, including the BSA, so that bad actors could create accounts, engage in cryptocurrency transactions, and deposit and withdraw cryptocurrency. As a direct result of their conspiracy and fraudulent scheme, bad actors laundered cryptocurrency that was taken from Plaintiffs and the Class as a result of hacks, ransomware attacks, and theft, through KuCoin.

The KuCoin Crypto-Wash Enterprise

169. KuCoin was founded in 2017 and since then has operated the cryptocurrency trading platform located at KuCoin.com and through smartphone apps. At all times relevant herein, KuCoin has been owned and operated by and through one or more associated companies, including defendants Peken Global, Mek Global, PhoenixFin, and Flashdot.

170. Flashdot is a company incorporated in the Cayman Islands and, during much of the Class Period, was the holding company of the KuCoin cryptocurrency trading platform.

171. Peken Global is a corporation under the laws of the Republic of Seychelles and has operated KuCoin since in or about September 2019. According to the NYAG Consent Order, Peken Global is the current owner of the KuCoin cryptocurrency trading platform. Peken Global is a subsidiary or affiliate of Flashdot.

172. PhoenixFin is incorporated under the laws of Singapore and operated KuCoin from about September 2017 through in or about December 2018. According to the CFTC Complaint, from at least July 2019 until at least June 2023, PhoenixFin was the owner of the "kucoin.com" domain. PhoenixFin is a subsidiary or affiliate of Flashdot.

173. Mek Global is incorporated under the laws of the Republic of Seychelles. At times relevant during the Class Period, KuCoin was operated by Mek Global along with Flashdot and its affiliated companies.

174. Defendants Gan, Tang, and others co-founded KuCoin.

175. Gan and Tang collectively own approximately 75% of the shares in Flashdot, the holding company for KuCoin.

176. Gan and Tang are the sole shareholders of Peken Global and have controlled Peken Global at all times relevant herein. Gan is Peken Global's Director.

177. As of in or about May 2018, Gan was the CEO of PhoenixFin, and Tang was its President.

178. Gan and Tang have directly or indirectly owned the various entities that collectively operate KuCoin. Defendants Gan and Tang, through their ownership of KuCoin and positions of authority at the entities in control of KuCoin, exercised substantial control over the affairs of the KuCoin Crypto-Wash Enterprise. They made the strategic decisions for KuCoin and exercised day-to-day control over its operations and finances. Additionally, in their pursuit of maximizing revenues and market share, Gan and Tang oversaw and directed KuCoin's strategy of willfully disregarding U.S. KYC and AML laws and regulations so that customers could use KuCoin anonymously and from the United States. By refusing to implement these necessary policies and procedures, the KuCoin Defendants, under the guise of a 'legitimate' cryptocurrency exchange, willfully encouraged and permitted bad actors to launder stolen cryptocurrency through the KuCoin platform.

179. Defendant Chainalysis, a Delaware corporation headquartered in New York, New York, is a crypto-tracing analysis company that was retained by KuCoin throughout the Class Period to implement Chainalysis' proprietary KYT software to identify and purportedly block money laundering and other illicit actions at KuCoin in real-time. Chainalysis also used its proprietary Reactor software to conduct further investigations into suspicious activities on the KuCoin platform.

KuCoin characterized its dealings with Chainalysis as a partnership to further deepen KuCoin's commitment to security and compliance. KuCoin highlighted its partnership with Chainalysis to make it appear as though KuCoin was committed to complying with the law when Defendants knew that was not true. KuCoin's statements about its partnership with Chainalysis provided KuCoin cover from scrutiny by regulators.

180. Defendant Chainalysis, *inter alia*, tracked transactions associated with blacklisted wallets (flagged as previously involved in potentially illicit or fraudulent activity) on KuCoin's platform using Chainalysis' software. KuCoin purportedly used Chainalysis' KYT software "to expose and block money laundering and other illicit actions in real-time and further deepen KuCoin's commitment to security and compliance." Chainalysis' KYT platform also provided KuCoin with alerts that "detect as much high risk cryptocurrency activity as possible with fewer false positives." As a result of the partnership between Chainalysis and KuCoin, Defendants knew of, or willfully ignored, obvious red flags and illicit transactions.

181. Even though Chainalysis provided KuCoin with software, information, and alerts to prevent bad actors from laundering crypto at the KuCoin exchange, the KuCoin Defendants refused to implement the policies or procedures necessary to stop or catch the bad actors. In reality, as both the KuCoin Defendants and Chainalysis were aware, even though KuCoin had access to information and red flags alerting KuCoin to potential crypto laundering and other illicit activities, KuCoin refused to implement adequate KYC and AML policies and procedures or dedicate resources to attempt to prevent those activities. They also knew that KuCoin was a magnet and hub for bad actors to launder cryptocurrency. Chainalysis was complicit with the KuCoin Defendants' refusal to prevent money laundering on the KuCoin platform in order to maintain the benefits of its partnership

with KuCoin. Chainalysis reaped substantial financial benefits from its partnership with KuCoin, including as the result of fees and revenues generated by the KuCoin Crypto-Wash Enterprise.

182. The KuCoin Defendants, despite being members of the CDA, permitted KuCoin deposit addresses blacklisted by the CDA to continue transacting on the KuCoin platform after the date of blacklisting. In many instances, the KuCoin Defendants permitted these blacklisted deposit addresses to continue using the platform for years after the deposit addresses were blacklisted.

183. Defendants Gan, Tang, Flashdot, Peken Global, PhoenixFin, Mek Global, including the KuCoin platform, and Chainalysis, constituted an "enterprise" (the "KuCoin Crypto-Wash Enterprise") within the meaning of 18 U.S.C. §1961(4) since the start of the Class Period, through which Defendants conducted the pattern of racketeering activity described herein, the activities of which affected interstate commerce.

184. Alternatively, defendants Gan, Tang, Flashdot, Peken Global, PhoenixFin, Mek Global, including the KuCoin platform, and Chainalysis, were associated-in-fact for a number of common and ongoing purposes, including executing and perpetrating the scheme alleged herein, and constituted an "enterprise" within the meaning of 18 U.S.C. §1961(4).

185. The activities of the KuCoin Crypto-Wash Enterprise affected interstate commerce because they involved commercial and financial activities across state lines, including through the operation of a website over the Internet, the operation of smartphone apps, and the transmission of cryptocurrency to, from, and within accounts at KuCoin. Users of the KuCoin exchange platform accessed it from around the United States and other locations in the world.

186. Defendants Gan, Tang, Flashdot, Peken Global, PhoenixFin, Mek Global, and Chainalysis exercised control over and directed the affairs of the KuCoin Crypto-Wash Enterprise

through, among other things, using KuCoin's senior management group and employees to direct critical aspects of the KuCoin Crypto-Wash Enterprise operations, including the following:

(a) structuring KuCoin's platform to enable users located in the United States to register and use KuCoin and without requiring that those users provide KYC information;

(b) actively marketing to users based in the United States, including with an affiliate program, even though Defendants knew that KuCoin lacked adequate KYC or AML policies;

(c) retaining a marketing firm in Canada to target users in the United States;

(d) causing KuCoin to participate in cryptocurrency conferences in the United States to acquire U.S.-based users, including a cryptocurrency conference held in New York, New York in or about June 2022;

(e) from at least in or about October 2018 through at least in or about March 2022, the domain "kucoin.com" was registered by Tang on behalf of PhoenixFin;

(f) in or about January 2018, Gan opened an account with a third-party customer service software provider on behalf of KuCoin, and the third party's software and services were thereafter used to provide KuCoin customer service to U.S. customers;

(g) from at least in or about July 2019 through the present, defendants Gan, Tang, Flashdot, Peken Global, PhoenixFin, and Mek Global caused KuCoin to allow customers who resided in the United States to anonymously obtain or maintain access to KuCoin, and to use spot, derivative, and margin trading services; and

(h) in or about November 2022, the KuCoin Defendants allowed a customer located in New York, New York, who was using a computer associated with a U.S. IP address, to

create anonymously a KuCoin account that provided access to KuCoin's spot, derivative, and margin trading services.

187. The KuCoin Crypto-Wash Enterprise constituted a single "enterprise" or multiple enterprises within the meaning of 18 U.S.C. §1961(4), as individuals and other entities associated-in-fact for the common purpose of engaging in Defendants' profit-making scheme.

188. The KuCoin Crypto-Wash Enterprise was an ongoing and continuing organization consisting of legal entities, as well as individuals, associated for the common or shared purpose of ensuring that KuCoin did not implement adequate KYC or AML policies so that KuCoin could generate massive fees and liquidity from the maximum number of people and increase market share, in violation of the law.

189. The KuCoin Crypto-Wash Enterprise functions by enabling crypto exchange transactions and other services. Many customers were not bad actors and used the KuCoin platform for legitimate purposes. However, Defendants, through the KuCoin Crypto-Wash Enterprise, have engaged in a pattern of racketeering activity that enabled bad actors to use KuCoin to launder stolen cryptocurrency so that it could not be tracked or recovered.

190. The KuCoin Crypto-Wash Enterprise engages in and affects interstate commerce because it involves commercial and financial activities across state boundaries, such as through the operation of KuCoin.com over the Internet and through the transmission of cryptocurrency into and out of KuCoin, and over KuCoin's exchange.

191. At all relevant times herein, each participant in the KuCoin Crypto-Wash Enterprise was aware of the scheme.

192. Defendants were each knowing and willing participants in the scheme and reaped revenues and/or profits therefrom.

193. The KuCoin Crypto-Wash Enterprise has an ascertainable structure separate and apart from the pattern of racketeering activity in which Defendants engaged. The KuCoin Crypto-Wash Enterprise is separate and distinct from each of the Defendants.

RICO Conspiracy

194. Defendants have not undertaken the practices described herein in isolation, but as part of a common scheme and conspiracy.

195. Defendants have engaged in a conspiracy to maximize revenues and/or market share for Defendants and their unnamed co-conspirators through the scheme alleged herein.

196. The objectives of the conspiracy are: (i) to execute the scheme; (ii) to enable customers to use KuCoin without requiring KYC or implementing AML policies, including U.S.-based users; and (iii) to gain market share and maximize fees and liquidity.

197. To achieve these goals, Defendants willfully disregarded U.S. laws and regulations and encouraged bad actors to launder crypto at KuCoin.

198. Defendants have also agreed to participate in other illicit and fraudulent practices, all in exchange for agreement to, and participation in, the conspiracy.

199. Each defendant and member of the conspiracy, with knowledge and intent, has agreed to the overall objectives of the conspiracy and participated in the common course of conduct to enable bad actors to launder crypto at KuCoin in order to reap transaction fees.

200. Because of Defendants' illegal scheme and conspiracy, Plaintiffs and the putative Class herein had crypto taken from them as a result of hacks, ransomware, or theft, laundered at KuCoin. Defendants' willful refusal to implement KYC and AML policies and procedures directly enabled the bad actors to launder Plaintiffs' and Class members' crypto and evade detection.

201. Throughout its partnership with KuCoin, Chainalysis advertised that its KYT protocol and other tools "can equip law enforcement and compliance with the tools they need to continue

tracing funds even when they move to DeFi protocols." Moreover, Chainalysis touted that it provided numerous tools that help exchanges and law enforcement "identify, trace, and seize crypto assets effectively." For example, Chainalysis provided a tool called "Wallet Scan," which it claims "revolutionizes wallet recovery by automating the discovery of derivation paths. This eliminates the need to manually reconstruct wallets, allowing investigators to focus on recovering assets instead." Similarly, Chainalysis offered "Chainalysis Reactor," which "enables investigators to follow the money wherever it leads. Even when the funds have been obscured or withdrawn, Reactor helps investigators track assets across blockchains, identify on- and off-ramps, and uncover real-world identities vital intelligence for building cases."

202. KuCoin publicly highlighted its partnership with Chainalysis to make it appear as if it complied with KYC and AML rules and regulations even though the KuCoin Defendants and Chainalysis knew that KuCoin failed to implement them. Although KuCoin had access to red flags that warned the KuCoin Defendants of potentially illicit transactions, the KuCoin Defendants ignored those red flags. By ignoring the red flags, including those provided by Chainalysis, the KuCoin Defendants willfully permitted bad actors to launder ill-gotten crypto through the KuCoin platform, despite having the means of identifying and halting the illicit activity, or, at a minimum, implementing policies and procedures that would have enabled victims and the authorities to track the stolen assets. Despite the fact that KuCoin categorically failed to utilize Chainalysis' tools to prevent money laundering and other illicit activity, Chainalysis continued its partnership with KuCoin in order to reap the financial and marketing benefits of the partnership.

203. But for Defendants' scheme, Plaintiffs and the putative Class herein would have been able to track and potentially recover their stolen crypto. Therefore, the damages that Defendants caused Plaintiffs and the putative Class herein may be measured by the dollar value of the

cryptocurrency taken from them as the result of illegal conduct, such as hacks, ransomware, or theft, which was laundered through KuCoin. At a minimum, damages may be measured by the value of the harm suffered by Plaintiffs and the members of the Class as a result of their inability to continue tracking the location of their stolen cryptocurrency assets and the loss of the potential recovery of those assets.

Pattern of Racketeering Activity

204. Defendants, each of whom is a person or entity associated-in-fact with the KuCoin Crypto-Wash Enterprise, knowingly, willfully, and unlawfully conducted or participated, directly or indirectly, in the affairs of the enterprise through a pattern of racketeering activity within the meaning of 18 U.S.C. §§1961(1), 1961(5), and 1962(c). The racketeering activity was made possible by Defendants' regular and repeated use of the facilities, services, distribution channels, and employees of the KuCoin Crypto-Wash Enterprise.

205. Defendants each committed multiple "Racketeering Acts," as described herein, including aiding and abetting such acts.

206. The Racketeering Acts were not isolated, but rather were related in that they had the same or similar purposes and results, participants, victims, and methods of commission. Further, the Racketeering Acts were continuous, occurring on a regular, and often daily, basis beginning in 2017 and continuing until at least 2024 (when Plaintiff Supples' crypto was laundered at KuCoin), and the harm of those Racketeering Acts continues today.

207. Defendants participated in the operation and management of the KuCoin Crypto-Wash Enterprise by directing its affairs, as described above.

208. In devising and executing the scheme to enable KuCoin to be used by anonymous customers and U.S.-based customers, including bad actors laundering cryptocurrency, Defendants, *inter alia*: (i) committed, and aided and abetted, acts constituting indictable offenses under 18 U.S.C.

§1960 (relating to illegal money transmitters) and 18 U.S.C. §1961(1)(E) (act indictable under the Currency and Foreign Transactions Reporting Act a/k/a the BSA); and (ii) aided and abetted acts constituting indictable offenses under 18 U.S.C. §1956 (laundering of monetary instruments), 18 U.S.C. §1957 (engaging in monetary transactions in property derived from specified unlawful activity), and 18 U.S.C. §2314 (relating to interstate transportation of stolen property). For the purpose of executing the scheme to maximize revenues and market share for KuCoin in violation of KYC and AML rules and regulations, Defendants committed these Racketeering Acts, which number in the millions, intentionally and knowingly with the specific intent to advance the illegal scheme.

209. Defendant Peken Global pled guilty to operating an unlicensed MTB in violation of 18 U.S.C. §1960. Similarly, as part of their deferred prosecution agreement, defendants Gan and Tang admitted that they "violated Title 18, United States Code, Sections 1960(a) and (b)(1)(A) and (B)" by "knowingly own[ing] . . . part of a money transmitting business that was not registered or licensed in the United States."

210. Defendants committed, and aided and abetted, acts constituting indictable offenses under 18 U.S.C. §1960 (relating to illegal money transmitters) and the BSA as follows:

(a) Defendants understood that KuCoin was an MTB from its launch in 2017 until at least December 2023 and was required to register with the U.S. Department of the Treasury's FinCEN and, since in or about July 2019, when KuCoin launched a derivatives trading platform, it has been an FCM. As a result, KuCoin was required to comply with the provisions of the BSA, 31 U.S.C. §5311 *et seq*., applicable to MTBs and FCMs, including implementing an effective AML program. Nevertheless, KuCoin did not register with FinCEN as an MTB or implement an effective AML program. In fact, Defendants willfully violated the BSA by enabling and causing KuCoin to

have an ineffective AML program, including a failure to collect or verify KYC information from a large portion of its users.

(b) As part of the willful evasion of KuCoin's obligations to comply with U.S. AML and KYC requirements, defendants Gan, Tang, Flashdot, Peken Global, PhoenixFin, and Mek Global affirmatively attempted to, and did, conceal the existence of KuCoin's large base of U.S. customers to make it appear as if KuCoin was exempt from U.S. AML and KYC requirements. Among other things, KuCoin actively prevented U.S. customers from even identifying themselves as such to KuCoin when establishing accounts and lied to at least one investor regarding the geographic location of its customers, falsely representing that it had no U.S. customers, when in truth and fact, KuCoin and its executives, including Gan and Tang, as well as Chainalysis, each knew that KuCoin's customer base included a substantial portion of U.S.-based customers.

(c) Defendants Gan, Tang, Flashdot, Peken Global, PhoenixFin, and Mek Global willfully conducted, and conspired to conduct, KuCoin as an unlicensed MTB from KuCoin's launch in 2017 to at least December 2023 in violation of 18 U.S.C. §§1960(a) and (b)(1)(B), and from July 2019 failed to register with FinCEN and Defendants failed to maintain an effective AML program in violation of the BSA, including 31 U.S.C. §§5318(h) and 5322. The KuCoin Defendants admitted to engaging in such conduct, as defendant Peken Global pled guilty to violating 18 U.S.C. §1960; and defendants Gan and Tang admitted their conduct violated 18 U.S.C. §1960.

(d) KuCoin was required to develop, implement, and maintain an effective AML program that was reasonably designed to prevent KuCoin from being used to facilitate money laundering and the financing of terrorist activities, and defendants KuCoin, Gan, Tang, and Chainalysis willfully failed to do so in violation of 31 U.S.C. §5318(h)(1) and 31 C.F.R. §1022.210. Additionally, KuCoin was required to accurately and timely report suspicious transactions to

FinCEN, and defendants KuCoin, Gan, Tang, and Chainalysis willfully failed to do so in violation of 31 U.S.C. §5318(g) and 31 C.F.R. §§1022.320 and 1026.320.

(e) Defendants Gan, Tang, Flashdot, Peken Global, PhoenixFin, Mek Global, and Chainalysis aided and abetted KuCoin's conduct as an unlicensed MTB in violation of 18 U.S.C. §§1960(a) and (b)(1)(B), and aided and abetted KuCoin's failure to implement and maintain an effective AML program in violation of the BSA, including 31 U.S.C. §§5318(h) and 5322.

(f) These Racketeering Acts were not isolated, but rather were related in that they had the same or similar purposes and results, participants, victims, and methods of commission. For years, KuCoin sought and obtained a substantial number of U.S.-based customers without requiring KYC information. For example, as revealed in the NYAG Consent Order, on or about December 12, 2023, more than 150,000 users in New York alone had accounts with KuCoin with assets valued at more than $16.7 million.

(g) As a result of the KuCoin Defendants' purposeful failure to implement adequate controls requiring KYC and AML policies and blocking transactions by bad actors, Gan, Tang, and KuCoin willfully enabled bad actors to launder cryptocurrency at KuCoin. For example, since its founding in 2017, KuCoin has received over $5 billion, and sent over $4 billion, of suspicious and criminal proceeds.

211. Additionally, Defendants aided and abetted acts constituting indictable offenses under 18 U.S.C. §1956 (laundering of monetary instruments), 18 U.S.C. §1957 (engaging in monetary transactions in property derived from specified unlawful activity), and 18 U.S.C. §2314 (relating to interstate transportation of stolen property) as follows:

(a) Defendants' scheme of maximizing revenues from all customers, including bad actors, by failing to implement KYC and AML procedures for KuCoin, turned KuCoin into a

hub and magnet for criminals and other bad actors to launder cryptocurrency. Operating KuCoin as a means to launder cryptocurrency aided and abetted cryptocurrency laundering by bad actors.

(b) Since approximately 2017, KuCoin processed billions of dollars in transactions by bad actors who took cryptocurrency from Plaintiffs and the putative Class herein as a result of hacks, ransomware attacks, or theft and utilized KuCoin to launder the cryptocurrency and/or to transfer the cryptocurrency through their KuCoin accounts and out of KuCoin in violation of 18 U.S.C. §1956 (laundering of monetary instruments) and 18 U.S.C. §1957 (engaging in monetary transactions in property derived from specified unlawful activity). Additionally, the illegally obtained cryptocurrency was transported, transmitted, or transferred in interstate or foreign commerce to or from KuCoin violation of 18 U.S.C. §2314 (relating to interstate transportation of stolen property). Defendants Gan, Tang, Flashdot, Peken Global, PhoenixFin, Mek Global, and Chainalysis aided and abetted those actions constituting indictable offenses.

(c) These Racketeering Acts were not isolated, but rather were related in that they had the same or similar purposes and results, participants, victims, and methods of commission.

212. Defendants and third parties have exclusive custody or control over the records reflecting the precise dates, locations, and details of the millions of transactions at KuCoin constituting the Racketeering Acts in violation of 18 U.S.C. §1960 (relating to illegal money transmitters), 18 U.S.C. §1961(1)(E) (act indictable under the Currency and Foreign Transactions Reporting Act a/k/a the BSA), 18 U.S.C. §1956 (laundering of monetary instruments), 18 U.S.C. §1957 (engaging in monetary transactions in property, derived from specified unlawful activity), and 18 U.S.C. §2314 (relating to interstate transportation of stolen property).

213. Because of the willful failure of KuCoin, Gan, and Tang to implement AML and KYC programs in violation of law, including the BSA, KuCoin, with the assistance of Chainalysis,

became a hub and magnet for bad actors to launder the proceeds of suspicious and criminal activities, including proceeds from hacks, ransomware, and theft. The KuCoin Defendants' willful refusal to implement KYC and AML policies and procedures directly enabled bad actors to launder crypto stolen from Plaintiffs and the members of the Class. Additionally, the KuCoin Defendants' willful refusal to implement KYC and AML policies and procedures directly led to the loss of the Plaintiffs' and the members of the Class's ability to locate and potentially recover some, if not all, of their stolen cryptocurrency laundered through KuCoin. As a result, Defendants' conduct as alleged herein led directly to the injuries suffered by Plaintiffs and the members of the Class.

CLASS ACTION ALLEGATIONS

214. Plaintiffs bring this action individually and as a class action pursuant to Federal Rule of Civil Procedure 23 on behalf of the following Class:

> All persons or entities in the United States whose cryptocurrency was removed from a digital wallet, account, or protocol as a result of a hack, ransomware attack, or theft, and, between August 21, 2020 and the date of Judgment (the "Class Period"), transferred to a KuCoin account, and who have not recovered some, if not all, of their cryptocurrency that was transferred to KuCoin (the "Class").

215. Excluded from the proposed Class are Defendants and co-conspirators, and their officers, directors, agents, trustees, parents, corporations, trusts, representatives, employees, principles, partners, joint ventures, and entities controlled by Defendants; their heirs, successors, assigns, or other persons or entities related to, or affiliated with, Defendants; and the judge(s) assigned to this action; and any member of their immediate families. Also excluded from the proposed Class are any persons or entities that engaged in the hack, ransomware attack, or theft, which resulted in the removal of Class members' cryptocurrency, or any persons or entities that transferred the cryptocurrency to KuCoin.

216. Subject to additional information obtained through further investigation and discovery, the foregoing definition of the Class may be expanded or narrowed by amendment, amended complaint, or at class certification proceedings.

217. **Numerosity**: Class members are so numerous that joinder of all individual members is impracticable. While the exact number and identities of Class members are unknown to Plaintiffs at this time and can only be ascertained through appropriate discovery, Plaintiffs allege that the Class is comprised of hundreds or thousands of individual members geographically disbursed throughout the United States. The number of Class members and their geographical disbursement renders joinder of all individual members impracticable if not impossible. Upon information and belief, KuCoin and third parties, including firms such as Chainalysis, possess lists of wallet addresses that would enable Plaintiffs to identify crypto that has been taken from Plaintiffs and the Class as a result of a hack, ransomware attack, or theft and transferred to KuCoin by bad actors.

218. **Existence and Predominance of Common Questions**: There are questions of fact and law common to Plaintiffs and the Class that predominate over any questions affecting solely individual members of the Class including, *inter alia*, the following:

(a) whether the KuCoin Defendants knowingly failed to implement or maintain adequate KYC and AML policies;

(b) whether KuCoin, Gan, and Tang encouraged U.S.-based customers to use KuCoin;

(c) whether Defendants committed civil RICO violations pursuant to 18 U.S.C. §§1962(c)-(d);

(d) whether Defendants converted, or aided and abetted the conversion of, cryptocurrency stolen from Plaintiffs and the Class members;

(e) whether Plaintiffs and the Class members have been harmed and the proper measure of relief;

(f) whether Defendants' actions proximately caused harm to Plaintiffs and the Class members;

(g) whether Plaintiffs and the Class members are entitled to an award of damages, treble damages, and attorneys' fees and expenses; and

(h) whether Plaintiffs and the Class members are entitled to equitable relief, and if so, the nature of such relief.

219. **Typicality**: Plaintiffs' claims are typical of the claims of the members of the proposed Class. Plaintiffs and the Class members have been injured by the same wrongful practices of Defendants. Plaintiffs' claims arise from the same practices and conduct that give rise to the claims of all Class members and are based on the same legal theories.

220. **Adequacy**: Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs' claims are coextensive with, and not antagonistic to, the claims of the other Class members. Plaintiffs are willing and able to vigorously prosecute this action on behalf of the Class, and Plaintiffs have retained competent counsel experienced in litigation of this nature.

221. **Superiority**: A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members is relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against defendants. It would thus be virtually impossible for the Class members, on an individual basis, to obtain effective redress for the wrongs done to them. Furthermore, even if the Class members could afford such individualized litigation, the court system could not. Individualized litigation would create the danger of inconsistent or

contradictory judgments arising from the same set of facts. Individualized litigation would also increase the delay and expense to all parties and the court system from the issues raised by this action. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, economies of scale, and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

222. Adequate notice can be given to the Class members directly using information maintained in Defendants' and/or third-party records or through notice by publication.

COUNT I

Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. §§1962(c)-(d) Against All Defendants

223. Plaintiffs re-allege and adopt by reference the allegations above contained in ¶¶1-222, as if fully set forth herein.

224. This Count I is brought against defendants Flashdot, Peken Global, Mek Global, PhoenixFin, Gan, Tang, and Chainalysis.

225. Plaintiffs are not relying on any contracts or agreements entered into between KuCoin and any users of KuCoin to assert any claims alleged in this Count I, and none of Plaintiffs' claims in this Count I derive from the underlying terms of any such contracts or agreements.

226. This claim arises under 18 U.S.C. §§1962(c) and (d), which provide in relevant part:

> (c) It shall be unlawful for any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce, to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity . . . .
>
> (d) It shall be unlawful for any person to conspire to violate any of the provisions of subsection . . . (c) of this section.

227. At all relevant times, Defendants were "persons" within the meaning of 18 U.S.C. §1961(3), because each defendant was an individual or "capable of holding a legal or beneficial

interest in property." Defendants were associated with an illegal enterprise, as described herein, and conducted and participated in that enterprise's affairs though a pattern of racketeering activity, as defined by 18 U.S.C. §1961(5), consisting of numerous and repeated uses of the interstate wire communications to execute a scheme to operate KuCoin in violation of 18 U.S.C. §1962(c).

228. The KuCoin Crypto-Wash Enterprise was created and/or used as a tool to carry out the elements of Defendants' illicit scheme and pattern of racketeering activity.

229. The KuCoin Crypto-Wash Enterprise has ascertainable structures and purposes beyond the scope and commission of Defendants' predicate acts and conspiracy to commit such acts.

230. The enterprise is separate and distinct from Defendants.

231. The members of the RICO enterprise all had the common purpose to maximize KuCoin's (and Chainalysis') revenues and market share by running KuCoin, and enabling KuCoin to be run, as a crypto exchange with virtually non-existent KYC or AML policies to serve U.S.-based customers and customers from sanctioned jurisdictions, including bad actors who engaged in the laundering of cryptocurrency obtained as the result of hacks, ransomware attacks, and theft.

232. The KuCoin Crypto-Wash Enterprise has engaged in, and its activities affected, interstate and foreign commerce by operating a website on the Internet (KuCoin.com) that served customers located throughout the United States, and received and sent cryptocurrency throughout the United States and the world and operated a cryptocurrency exchange facilitating the exchange of cryptocurrency between users in the United States and around the world.

233. The KuCoin Crypto-Wash Enterprise actively disguised the nature of Defendants' wrongdoing and concealed or misrepresented Defendants' participation in the conduct of the KuCoin Crypto-Wash Enterprise to maximize profits and market share while minimizing their exposure to criminal and civil penalties.

234. Each of the Defendants exerted substantial control over the KuCoin Crypto-Wash Enterprise, and participated in the operation and managed the affairs of the enterprise as described herein.

235. Defendants have committed or aided and abetted the commission of at least two acts of racketeering activity, *i.e.*, indictable violations of 18 U.S.C. §§1960, 1961(1)(E), 1956, 1957, and 2314, within the past ten years. The multiple acts of racketeering activity that Defendants committed and/or conspired to, or aided and abetted in the commission of, were related to each other, began in 2017 and would have continued and posed a threat of continued racketeering activity if it were not for the DOJ and other actions against Defendants, and therefore constitute a "pattern of racketeering activity."

236. Even after the KuCoin Defendants belatedly adopted a KYC program for new customers in July 2023 the acts of racketeering activity continued. For example, cryptocurrency was transferred to KuCoin from the virtual currency mixer Tornado Cash through at least November 2023 and KuCoin actively served U.S. customers, including those located in New York, until at least December 2023, in violation of the BSA. Additionally, Plaintiff Supples had his stolen cryptocurrency laundered at KuCoin in December 2024.

237. Defendants' predicate acts of racketeering within the meaning of 18 U.S.C. §1961(1) include, but are not limited to:

(a) **Operated an Unlicensed MTB and Violated the BSA**: Defendants Gan, Tang, Flashdot, Peken Global, PhoenixFin, and Mek Global, aided and abetted by Chainalysis, conducted, and conspired to conduct, KuCoin as an unlicensed MTB from 2017 to at least July 2023 to December 2023 in violation of 18 U.S.C. §§1960(a) and (b)(1)(B), and the KuCoin Defendants, aided and abetted by Chainalysis failed to maintain an effective AML program, in violation of the

BSA, including, 31 U.S.C. §§5318(h) and 5322 until at least December 2024. Defendants willfully violated the BSA by causing KuCoin to have an ineffective AML program, including a failure to collect or verify KYC information from a large portion of its users.

(b) **Monetary Laundering and Transportation of Stolen Property**: KuCoin took custody of and processed millions of dollars in transactions by bad actors who took cryptocurrency from Plaintiffs and the Class through hacks, ransomware attacks, theft, and/or deceptive conduct and utilized KuCoin to remove the ability of Plaintiffs and members of the Class to track the crypto, and/or to transfer the crypto through their KuCoin accounts and/or out of KuCoin in violation of 18 U.S.C. §1956 (laundering of monetary instruments) and 18 U.S.C. §1957 (engaging in monetary transactions in property derived from specified unlawful activity). Additionally, the illegally obtained cryptocurrency was stolen from victims in the United States and transported, transmitted, or transferred in interstate or foreign commerce to or from KuCoin in violation of 18 U.S.C. §2314 (relating to interstate transportation of stolen property). Defendants aided and abetted those violations as alleged above.

238. Many of the precise dates and details of the illegal use of KuCoin to launder and transfer cryptocurrency cannot be ascertained without access to Defendants' books and records. Indeed, the success of Defendants' scheme depended upon secrecy, and Defendants have withheld details of the scheme from Plaintiffs and the Class members. Generally, however, Plaintiffs have described occasions on which the predicate acts alleged herein would have occurred. They include the transfer of millions of dollars in cryptocurrency over several years.

239. The KuCoin Defendants have obtained money and property belonging to Plaintiffs and the Class because of these statutory violations. Plaintiffs and the Class members have been

injured in their business or property by Defendants' overt acts, and by their aiding and abetting the acts of others.

240. In violation of 18 U.S.C. §1962(d), Defendants conspired to violate 18 U.S.C. §1962(c), as alleged herein. Various other persons, firms, and corporations, not named as defendants in this complaint, have participated as co-conspirators with Defendants in these offenses and have performed acts in furtherance of the conspiracy.

241. Each defendant aided and abetted violations of the above laws, thereby rendering them indictable pursuant to 18 U.S.C. §2 as if they were a principal in the 18 U.S.C. §§1960, 1961(1)(E), 1956, 1957, and 2314 offenses.

242. Plaintiffs and the Class have been injured in their property because of Defendants' violations of 18 U.S.C. §§1962(c) and (d), including the value of their cryptocurrency taken by bad actors that was transferred to KuCoin, as well as the value of the harm from the loss by Plaintiffs and Class members of the ability to track and identify the location of their stolen assets and potentially recover those assets. In the absence of Defendants' violations of 18 U.S.C. §§1962(c) and (d), Plaintiffs and the Class members would not have had their stolen crypto laundered through KuCoin such that the cryptocurrency was no longer traceable, and they had no chance to recover their stolen assets.

243. The injuries suffered by Plaintiffs and the Class were directly and proximately caused by Defendants' racketeering activity.

244. The KuCoin Defendants willfully violated the laws requiring KYC and AML policies and, along with Chainalysis, knew that bad actors were transferring crypto to and from KuCoin, and exchanging that crypto on KuCoin's exchange, and that, as a result, the crypto would no longer be traceable on the public blockchain, such that any chance of the recovery of those assets would be

lost. The KuCoin Defendants' violations of the laws requiring KYC and AML policies enabled bad actors to successfully complete and profit from the theft of crypto belonging to Plaintiffs and the members of the Class. Had the KuCoin Defendants complied with their obligations under the law, the bad actors would not have been able to launder the cryptocurrency stolen from Plaintiffs and the members of the Class at KuCoin.

245. Under the provisions of 18 U.S.C. §1964(c), Plaintiffs are entitled to bring this action and to recover treble damages, the costs of bringing this suit, and reasonable attorneys' fees. Defendants are accordingly liable to Plaintiffs and the Class members for three times their actual damages as proven at trial plus interest and attorneys' fees.

COUNT II

Conversion
Against the KuCoin Defendants

246. Plaintiffs re-allege and adopt by reference the allegations above contained in ¶¶1-166 and 214-222, as if fully set forth herein.

247. This Count II is brought against defendants Flashdot, Peken Global, Mek Global, PhoenixFin, Gan, and Tang (the KuCoin Defendants).

248. Plaintiffs are not relying on any contracts or agreements entered into between KuCoin and any users of KuCoin to assert any claims alleged in this Count II, and none of Plaintiffs' claims in this Count II derive from the underlying terms of any such contracts or agreements.

249. At the time their cryptocurrency was taken by bad actors by hacks, ransomware attacks, or theft, Plaintiffs and the Class owned and had the right to immediately possess the cryptocurrency in their respective private cryptocurrency wallets, protocols, and/or accounts at cryptocurrency exchanges other than KuCoin, not just a mere right to payment for the value of that cryptocurrency.

250. Plaintiffs and Class members also owned and had the right to immediately possess their stolen cryptocurrency that was later deposited into KuCoin addresses.

251. As can be done with Plaintiffs' specific, identifiable cryptocurrency, the Class members' cryptocurrency assets at issue are specific, identifiable property and can be traced to and from KuCoin accounts.

252. At all relevant times, the KuCoin Defendants knew that cryptocurrency stolen from Plaintiffs and the Class members had been transferred to accounts on KuCoin's exchange.

253. Because KuCoin had access to lists of blacklisted wallets designated by other exchanges and government authorities, the KuCoin Defendants had actual knowledge that cryptocurrency deposited into KuCoin by bad actors associated with these wallets was obtained through illicit or fraudulent means.

254. Notwithstanding the knowledge of the custody of stolen assets in a KuCoin account, the KuCoin Defendants accepted the receipt of the cryptocurrency of Plaintiffs and the members of the Class and benefitted from exchanging Plaintiffs' and the Class members' cryptocurrency for other cryptocurrency, thereby converting Plaintiffs' and the Class members' cryptocurrency. The KuCoin Defendants also benefitted from the liquidity generated on the KuCoin exchange as a result of the exchange of cryptocurrency stolen from Plaintiffs and the members of the Class.

255. The KuCoin Defendants permitted numerous CDA-blacklisted KuCoin deposit addresses to continue using the platform after the date of blacklisting, with one such deposit account receiving over 20,000 transfers valued at more than $2,300,000 after it was blacklisted.

256. The KuCoin Defendants knowingly maintained inadequate KYC and AML policies at KuCoin, which enabled cryptocurrency hackers and thieves to launder cryptocurrency through the

KuCoin ecosystem without providing valid or sufficient personal identification and proof of lawful possession of the cryptocurrency.

257. The KuCoin Defendants knew KuCoin's KYC and AML policies and procedures, including any tracing analysis of where funds originated, were nonexistent or inadequate. Nevertheless, those inadequacies were ignored, and no effort was taken to utilize reasonable measures to remedy those dangerous shortcomings.

258. As a result of the knowingly inadequate KYC and AML policies, the KuCoin Defendants were able to knowingly and unlawfully retain possession of stolen cryptocurrency, collect significant transaction fees, increase liquidity on the KuCoin exchange, and drive revenue and profits by furthering KuCoin's image as a promoter of anonymous and unregulated financial transactions, attracting bad actors, fraudsters, and other transacting parties seeking to evade scrutiny.

259. The KuCoin Defendants knew that they were in possession of stolen cryptocurrency because of, among other things, KuCoin's partnership with Chainalysis. KuCoin partnered with Chainalysis to implement KYT software "to expose and block money laundering and other illicit actions in real-time and further deepen KuCoin's commitment to security and compliance." Chainalysis' KYT platform provided KuCoin with alerts that "detect as much high risk cryptocurrency activity as possible with fewer false positives."

260. Plaintiffs and the Class are entitled to the value of their stolen cryptocurrency placed in KuCoin addresses and an amount of damages to be proven at trial, plus interest.

COUNT III

Aiding and Abetting Conversion
Against All Defendants

261. Plaintiffs re-allege and adopt by reference the allegations above contained in ¶¶1-166 and 214-222, as if fully set forth herein.

262. This Count III is brought against defendants Flashdot, Peken Global, Mek Global, PhoenixFin, Gan, Tang and Chainalysis.

263. Plaintiffs are not relying on any contracts or agreements entered into between KuCoin and any users of KuCoin to assert any claims alleged in this Count III, and none of Plaintiffs' claims in this Count III derive from the underlying terms of any such contracts or agreements.

264. At the time their cryptocurrency was taken by bad actors by hacks, ransomware attacks, or theft, Plaintiffs and the Class owned and had the right to immediately possess the cryptocurrency in their respective private cryptocurrency wallets, protocols, and/or accounts at cryptocurrency exchanges other than KuCoin, not just a mere right to payment for the value of that cryptocurrency.

265. As can be done with Plaintiffs' specific, identifiable cryptocurrency, the Class members' cryptocurrency assets at issue are specific, identifiable property and can be traced to and from KuCoin accounts.

266. At all relevant times, Defendants had actual knowledge that cryptocurrency taken from Plaintiffs and the Class members had been transferred to accounts on KuCoin's exchange.

267. Notwithstanding Defendants' actual knowledge of the custody of stolen assets in a KuCoin address, bad actors absconded with, and converted for their own benefit, Plaintiffs' and the Class members' property. Defendants substantially assisted and enabled bad actors to complete the conversion of the stolen cryptocurrency assets.

268. In many instances, the KuCoin Defendants and Chainalysis had actual knowledge that KuCoin permitted cryptocurrency to be transferred into KuCoin deposit addresses months or even years after the date of blacklisting, despite actual knowledge that these deposit addresses were reported to have been previously engaged in illicit activity.

269. Defendants rendered knowing and substantial assistance to cryptocurrency bad actors and thieves in their commission of conversion through which they obtained Plaintiffs' and the Class members' cryptocurrency, such that they culpably participated in the conversion.

270. Defendants knew that KuCoin ignored the law and maintained inadequate KYC and AML policies, which enabled cryptocurrency hackers and thieves to launder cryptocurrency through the KuCoin ecosystem without providing valid or sufficient personal identification and proof of lawful possession of the cryptocurrency.

271. Defendants knew that KuCoin's KYC and AML policies and procedures, including any tracing analysis of where funds originated, were nonexistent or inadequate. Nevertheless, they ignored those inadequacies and made no effort to utilize reasonable measures, including the KYT protocol provided by Chainalysis, to remedy those dangerous shortcomings. This amounts to "driving the getaway car" for the cryptocurrency thieves with full awareness of the harm being committed.

272. As a result of KuCoin's inadequate KYC and AML policies, KuCoin, Gan, and Tang were able to collect significant transaction fees, increase liquidity on the KuCoin exchange, and drive revenue and profits by furthering their image as promoters of anonymous and unregulated financial transactions, attracting bad actors, fraudsters, and other transacting parties seeking to evade scrutiny. Additionally, Chainalysis earned lucrative fees from KuCoin by tracking the illicit transactions and providing KuCoin access to red flags and other information showing illicit transactions flowed through KuCoin accounts. At the same time, Chainalysis knew that KuCoin did not use Chainalysis' software solutions or services to prevent the laundering of crypto and publicly highlighted its partnership with Chainalysis for appearances only. This, in turn, provided KuCoin

cover from scrutiny from regulators so that the KuCoin Defendants could continue to avoid complying with KYC and AML laws.

273. In effect, Defendants were consciously participating in the conversion of Plaintiffs' and the Class members' cryptocurrency, such that their assistance in the conversion was pervasive, systemic, and culpable.

274. Plaintiffs and the members of the Class are entitled to the value of their stolen cryptocurrency placed in KuCoin addresses and an amount of damages to be proven at trial, plus interest.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Sofia Reca and James K. Supples, individually and on behalf of all others similarly situated, respectfully pray for relief as follows:

A. Declaring that this action is properly maintainable as a class action and certifying Plaintiffs as the Class representatives and their counsel as Class counsel;

B. Declaring that Defendants committed civil RICO violations pursuant to 18 U.S.C. §§1962(c)-(d);

C. Declaring that the KuCoin Defendants' actions, as set forth above, converted Plaintiffs' and the Class members' cryptocurrency, or alternatively, that the Defendants aided and abetted conversion of that cryptocurrency, where they knew the KuCoin Defendants failed to follow KYC or AML laws;

D. Awarding Plaintiffs and the Class members actual, compensatory, and treble damages as allowed by applicable law;

E. Enjoining Defendants from continuing to commit the violations alleged herein, freezing all cryptocurrency in the KuCoin Defendants' possession that belong to Plaintiffs and the

Class, ordering the return of cryptocurrency taken from Plaintiffs and the Class, and ordering other necessary injunctive relief;

F. Awarding pre-judgment and post-judgment interest at the highest rate allowed by law;

G. Awarding costs, including experts' fees, and attorneys' fees and expenses, and the costs of prosecuting this action; and

H. Granting such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury, pursuant to Fed. R. Civ. P. 38(b), on all issues so triable.

DATED: April 14, 2025

ROBBINS GELLER RUDMAN
& DOWD LLP
SAMUEL H. RUDMAN
EVAN J. KAUFMAN
JONATHAN A. OHLMANN

/s/ Evan J. Kaufman
EVAN J. KAUFMAN

58 South Service Road, Suite 200
Melville, NY 11747
Telephone: 631/367-7100
631/367-1173 (fax)
srudman@rgrdlaw.com
ekaufman@rgrdlaw.com
johlmann@rgrdlaw.com

ROBBINS GELLER RUDMAN
& DOWD LLP
ERIC I. NIEHAUS (admitted *pro hac vice*)
655 W. Broadway, Suite 1900
San Diego, CA 92101
Telephone: 619/231-1058
619/231-7423 (fax)
ericn@rgrdlaw.com

SILVER MILLER
DAVID C. SILVER (admitted *pro hac vice*)
JASON S. MILLER (*pro hac vice* forthcoming)
4450 NW 126th Avenue, Suite 101
Coral Springs, FL 33065
Telephone: 954/516-6000
dsilver@silvermillerlaw.com
jmiller@silvermillerlaw.com

Attorneys for Plaintiffs